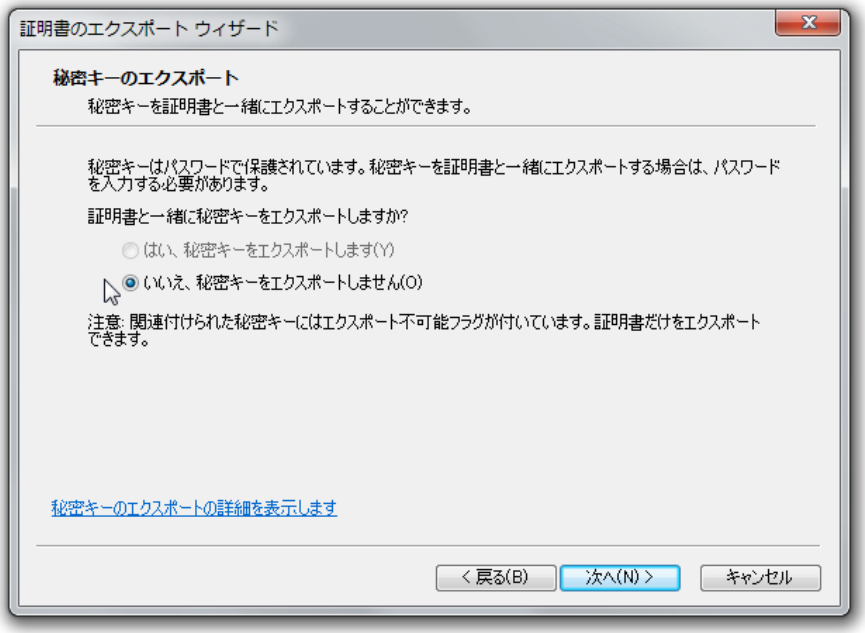
pkfcx

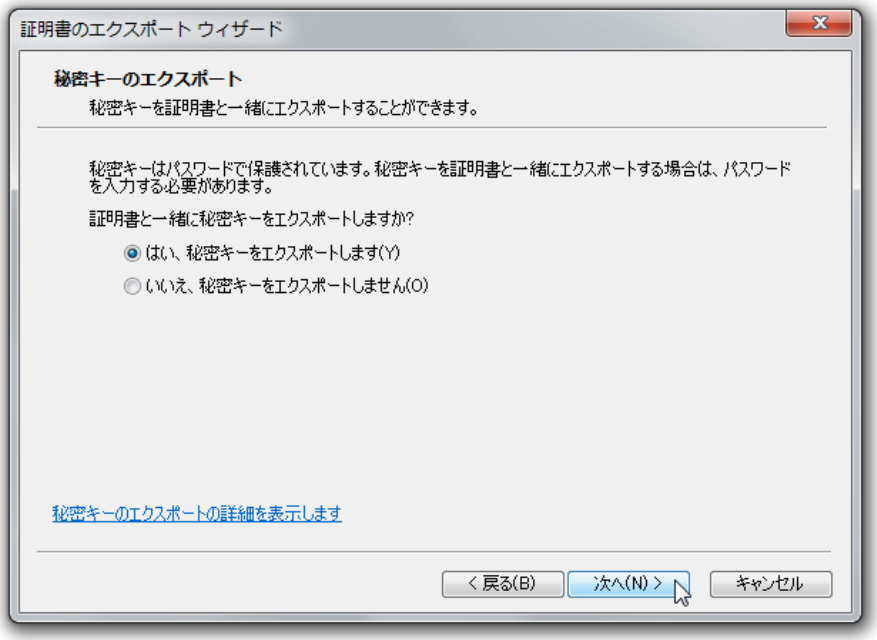
Private Key ForCe eXport

概要

本ソフトは、Windows インターネットバンキングで使われる電子証明書が「秘密鍵エクスポート不可」になっているため、これの完全バックアップが取れないとき、



これを強制的にエクスポート可能にして完全バックアップを取ります。



動作確認環境

Windows 環境でのみ動作します。以下の OS 環境であればそれ以上の動作要件はありません。

対応プラットフォーム x86(IA-32)と x64 (その他のプラットフォームには対応していません)

x86 環境

WindowsXP-SP3 Windows2003-R2-SP2 Windows2008-R1-SP2

Windows7 Windows7-SP1 Windows8 Windows8.1

x64 環境

Windows2008-R2-SP1 Windows7 Windows7-SP1 Windows8 Windows2012 Windows8.1 Windows10

(注意 x64 の WindowsXP では動きません)

これ以外の OS 環境では動きません。x64 環境で x86 版は(WOW64 でも)動作しません。

本ソフトは必ず書込み可能なドライブ・ディレクトリから起動してください。CD 等からは起動できません。

同梱ファイル

pkfcx本体 pkfcx32.exe (x86用実行ファイル) pkfcx64.exe (x64用実行ファイル)
pkfcx-mini本体 pkfcx-mini32.exe (x86用実行ファイル) pkfcx-mini64.exe (x64用実行ファイル)
その他説明書

インストール

インストール作業は不要です。実行ファイルを直接起動してください。
尚、バージョンアップ時には本ソフトを起動後一旦「完全終了」ボタンで終了してから再起動してください。

アンインストール

本ソフトは起動するとシステムのいくつかのレジストリを使用する他、テンポラリフォルダでいくつかのファイルを生成します。しかし「完全終了」ボタンを押して終了することでこれらを削除し導入前の環境に戻せます。
すなわちアンインストール作業は不要です。
「完全終了」ボタンによる終了は、原則本ソフトによるシステムへの残存物を全て削除しますが、
本ソフトが試用制限を設けている関係上、試用関係情報のみ例外としてシステムに残存させてもらっています。
尚、本ソフトの使用レジストリは以下で画面位置等を記録しています。

HKEY_LOCAL_MACHINE¥SOFTWARE¥pkfcx KEY_LOCAL_MACHINE¥SOFTWARE¥pkfcx_regist

HKEY_LOCAL_MACHINE¥SOFTWARE¥pkfcx_mini KEY_LOCAL_MACHINE¥SOFTWARE¥pkfcx_mini_regist

シェアウェア・試用について

本ソフトは起動回数「10 回まで」、インストール後「7 日間」試用することができる「シェアウェア」です。
その間で、お使いの環境での動作確認を行っていただき、継続使用する場合はご購入ください。
但し「秘密鍵強制エクスポート機能」以外は無償で継続使用できます。

金額・支払方法について

ソフト本体価格(消費税別)5,600 円です。支払方法は原則「ベクタシェアレジ」のみとなります。
ベクタシェアレジがなんらかの事情で利用できない方は下記メールアドレスへ連絡ください。
個別に折返し、銀行振込による方法をご連絡します。

連絡先

作者への連絡先は下記のとおりです。

ハンドル 丸太
メールアドレス qqcr2rd9k@arion.ocn.ne.jp

「pkfcx-mini」について

「pkfcx」が本体プログラム、「pkfcx-mini」が「pkfcx」の機能縮小版付属プログラムになります。
Ver1.8 以降の本ソフト購入者の方はこの両方を制限無しに使えますが、
試用制限解除の認証手続きはそれぞれ別途となりますのでご注意ください(後述)。

Ver1.7 までの「pkfcx」の購入者の方へ
　無料で「pkfcx-mini」の試用制限解除キーを取得できます
　上記「丸太」のメールアドレスまでご連絡ください。
　折返し、解除キーを送付いたします。

Ver1.7 までの「pkfcx-mini」の購入者の方へ
　差額(消費税別)4480 円にて「pkfcx」へのアップグレードを承ります。
　上記「丸太」のメールアドレスに、購入時の登録したメールアドレスとともにご連絡ください。
　折返し、今後の手続きの詳細をご連絡いたします。

対応暗号プロバイダ

「秘密鍵強制エクスポート機能」は以下の CSP に対応しています。

Microsoft Base Cryptographic Provider v1.0
Microsoft Strong Cryptographic Provider
Microsoft Enhanced Cryptographic Provider v1.0
Microsoft RSA Schannel Cryptographic Provider
Microsoft RSA Signature Cryptographic Provider
Microsoft Enhanced RSA and AES Cryptographic Provider
Microsoft Base DSS Cryptographic Provider
Microsoft Base DSS and Diffie-Hellman Cryptographic Provider
Microsoft DH Schannel Cryptographic Provider
Microsoft Enhanced DSS and Diffie-Hellman Cryptographic Provider

（Microsoft Base Smart Card Crypto Provider については対応していません。）

その他注意事項

① ドライブを暗号化するソフトで「システムドライブ」全体を暗号化してある場合「pkfcx」は試用回数及び期間の計測を誤り、初回起動時いきなり試用回数または期限超過になります。そのような環境では「試用」できないことをご了承ください。
② システムに、物理ハードディスクが最低 1 台接続されている必要があります。具体的には Windows システム上に「¥¥.¥PhysicalDrive0」のシンボリックリンクが存在している必要があります。

簡単「ネットバンキング電子証明書」バックアップ方法

ここでは仮に Windows7-SP1 x86 環境の例で説明します（他の環境では多少の違いがありますが同様です）。

ターゲット証明書の選択

本ソフトを起動します。
OS 起動後の本ソフト「初回起動時」は本ソフトによるシステム「調査」に時間が掛るため数秒から十数秒待機してください。画面左下にその旨表示されます。2 回目以降は待たされることはありません。

調査が終了すると以上のような画面が現れます。
ツリービュー内の「現在のユーザー」ノードの展開スイッチ(三角のしるし)をクリックして展開してください。

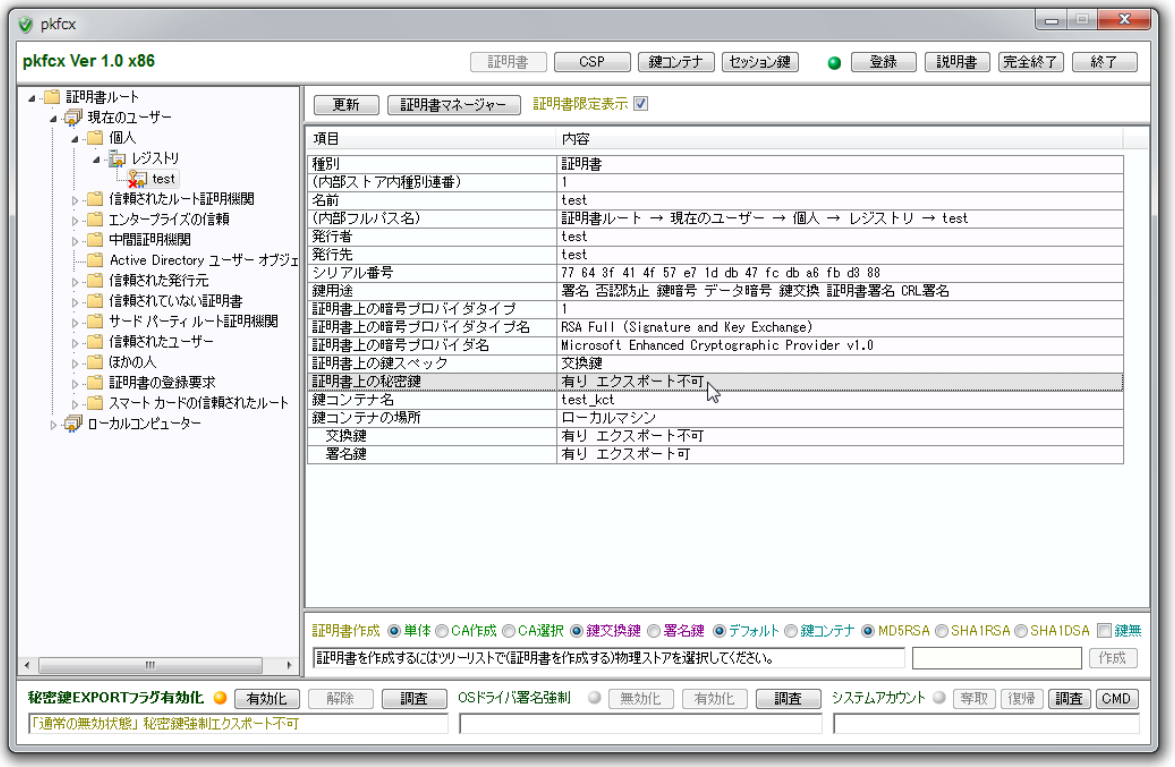
システムローケーション「現在のユーザー」内のシステムストアが列挙されますので、
「個人」のノードをクリックしてそのシステムストアを展開してください。

以上のようにそのシステム(論理)ストア内の物理ストアが展開されます。
ここでは「レジストリ」が出てきますのでそれを展開します。

このように「証明書」が列挙されます。例として「test」という名前の証明書が見えています。
ここでターゲットとなるネットバンキング用の電子証明書を選択してもらうことになりますが、
以降、説明のため「test」がターゲットとなる証明書と仮定して話を進めます。

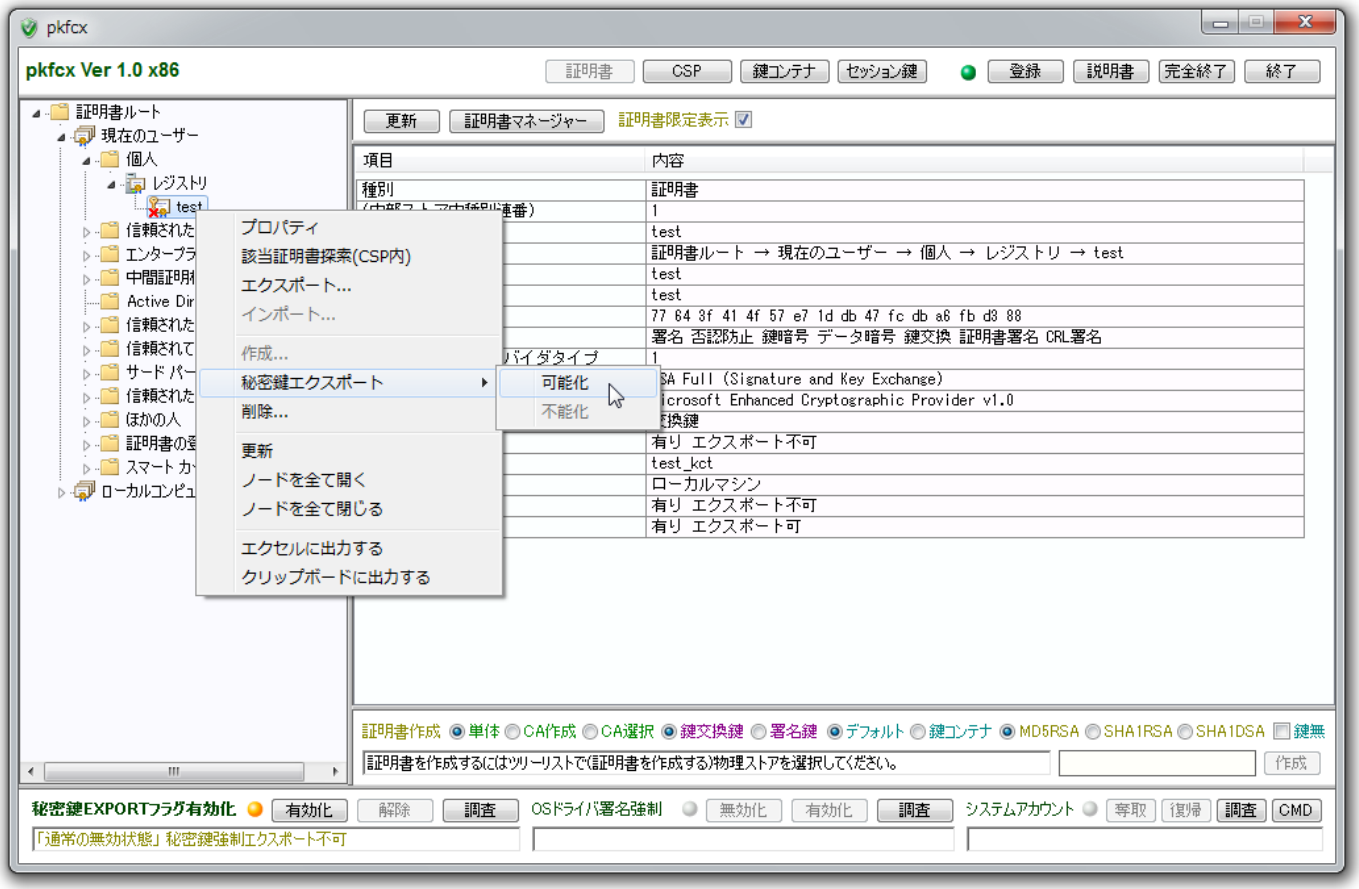
　ターゲットとなる証明書がわからない場合、通例その名前に関連する文字(金融機関名等)が入っていますのでそれを頼りに見つけてください。この説明では「現在のユーザー」「個人」にターゲット証明書があると仮定していますが、かならずしもそこにターゲットがあるとは限りませんので、みつからない場合は別の場所も探してください。

この「test」という証明書は、一般的なネットバンキング用電子証明書と同様に「秘密鍵エクスポート不可」になっています。これは以下のような情報から判別できます。
またツリービューノード上の「test」の左の小さいアイコンに小さい赤い「×」マークがありますが、これもそのことを示しています。

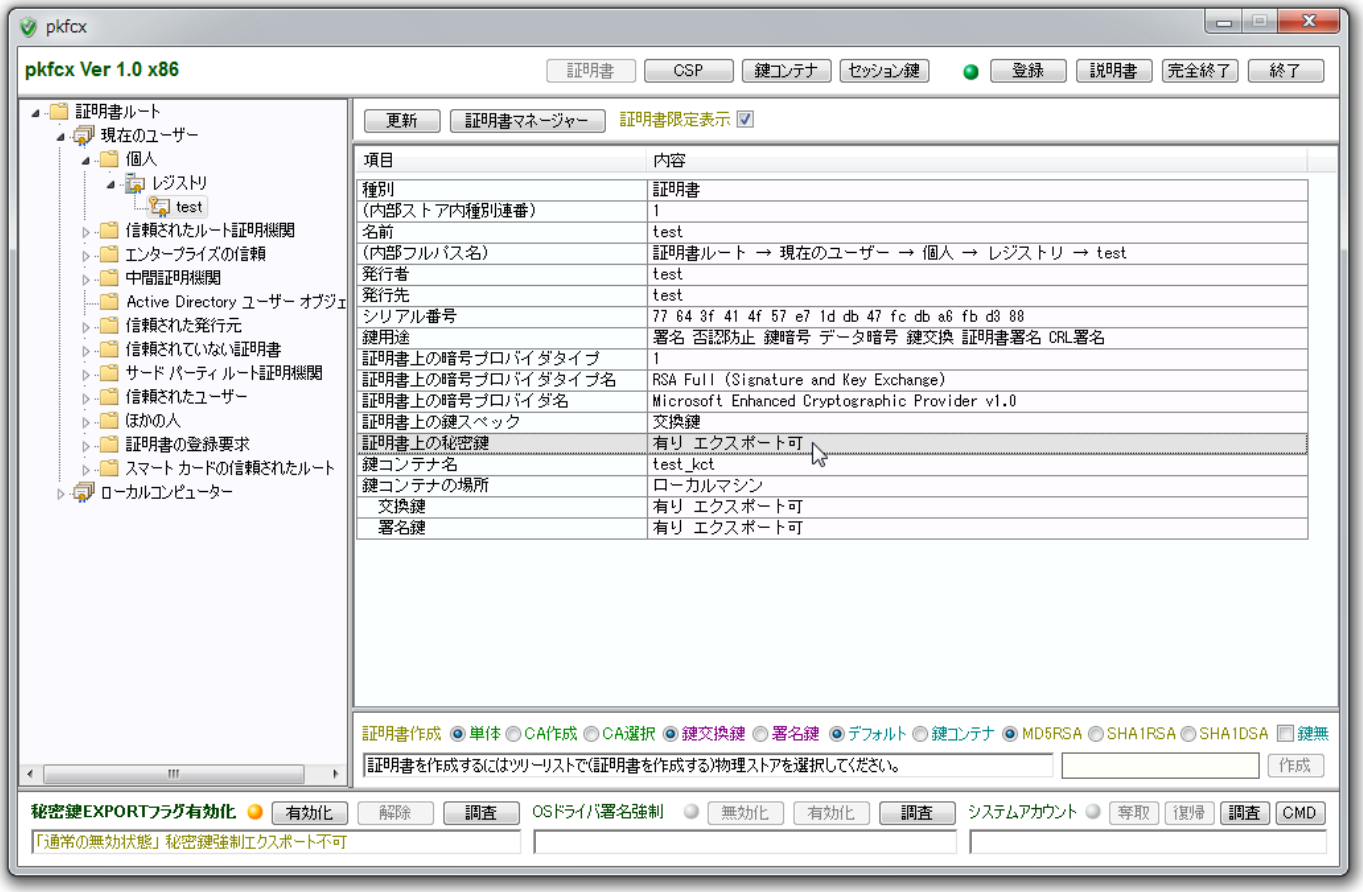


エクスポート可能化

次に、<u>秘密鍵エクスポート不可状態を解除してエクスポート可能化します</u>。
まずは証明書「test」のノード上でマウスを「右クリック」してコンテキストメニューを出してください。

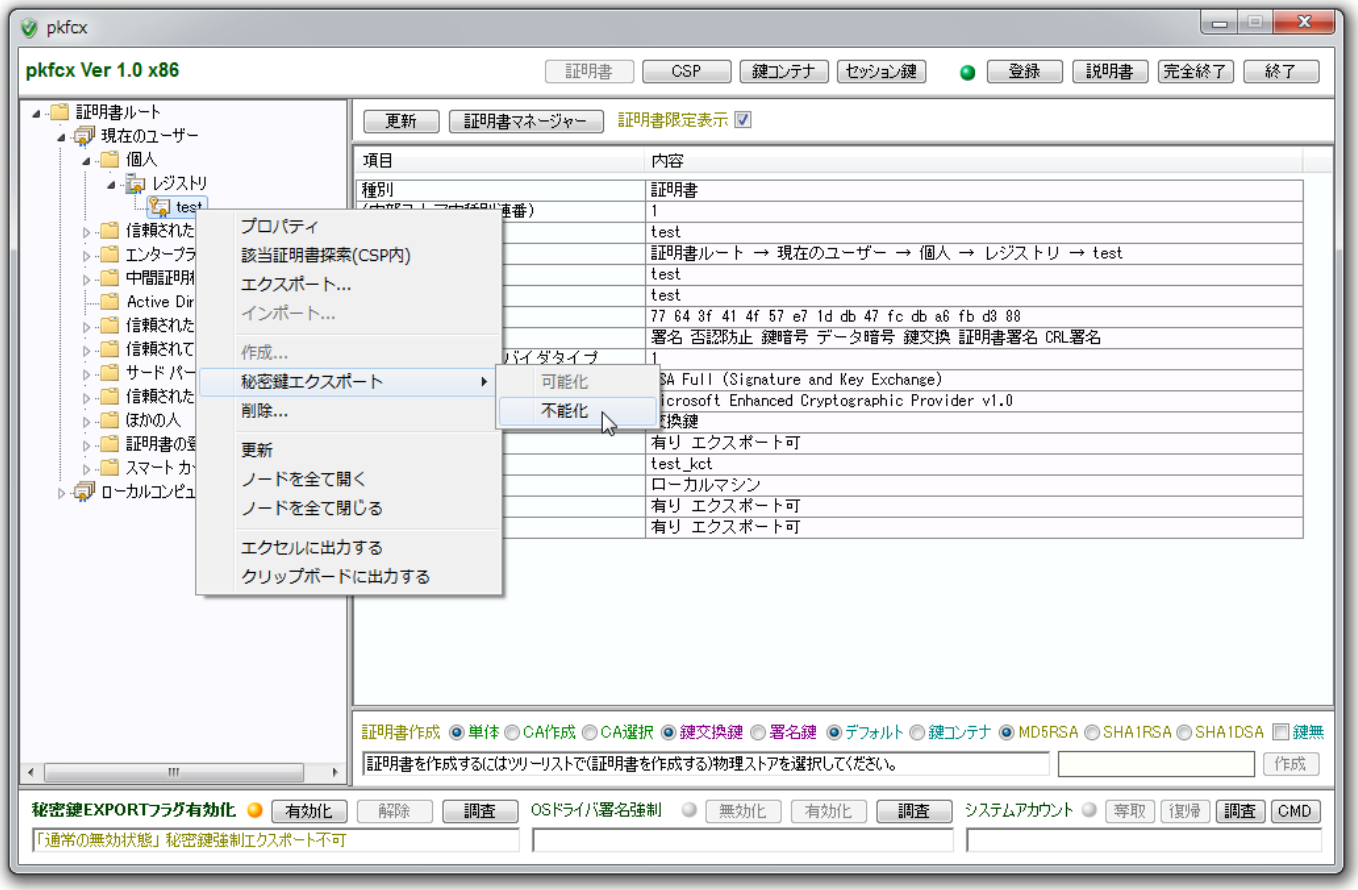


このように「秘密鍵エクスポート」メニュー項目内の「可能化」を選択しクリックしてください。
すると以下のようになります。

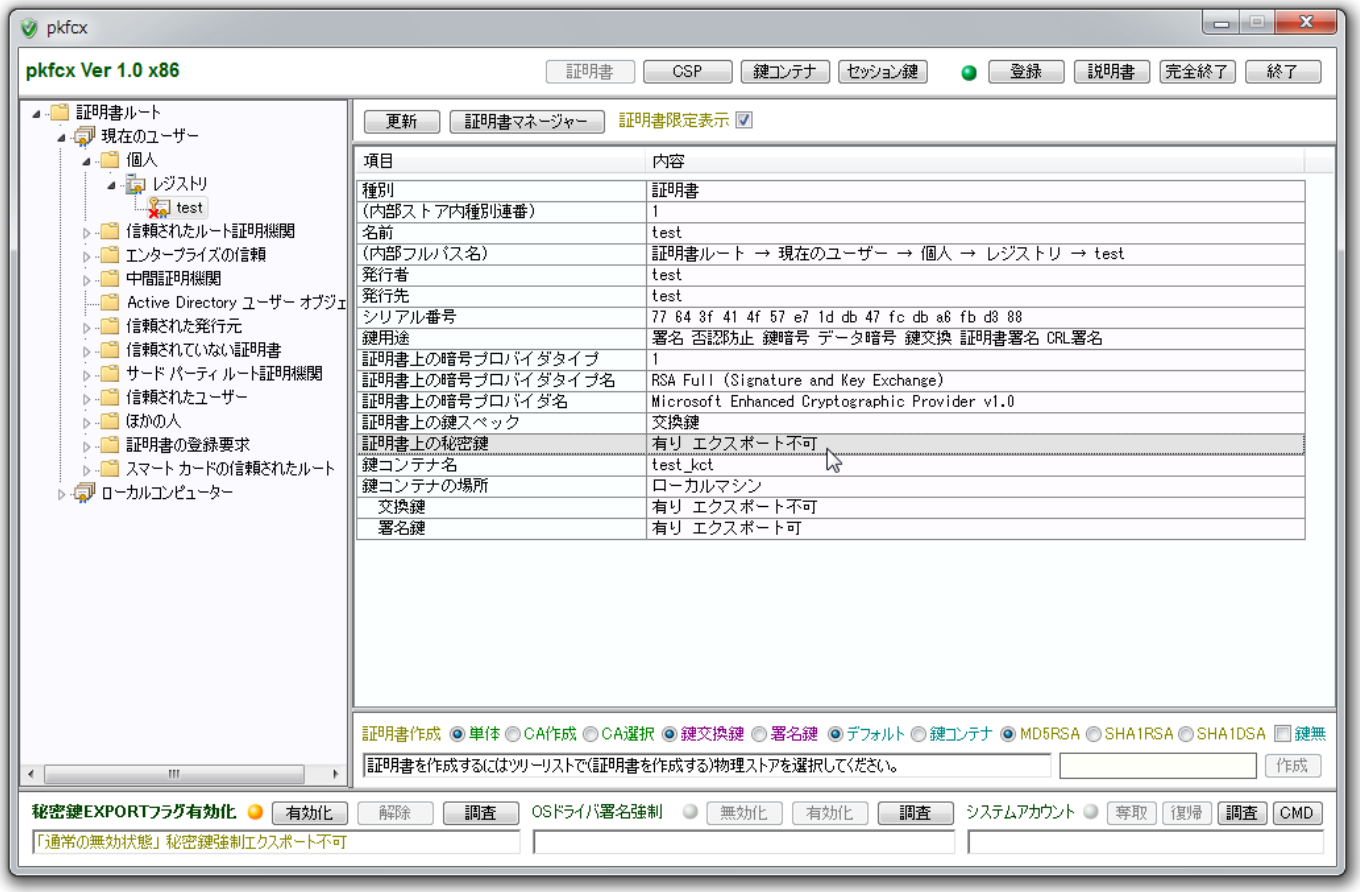


先ほど「エクスポート不可」となっていたところが「可」に変わり、
「test」の左のアイコンの赤い「×」マークも消えました。
これで「秘密鍵付きでエクスポート」すなわち「完全バックアップ」が取れるようになりました。

尚、ここで以下のように再度コンエテキストメニューを出し「不能化」をクリックすると

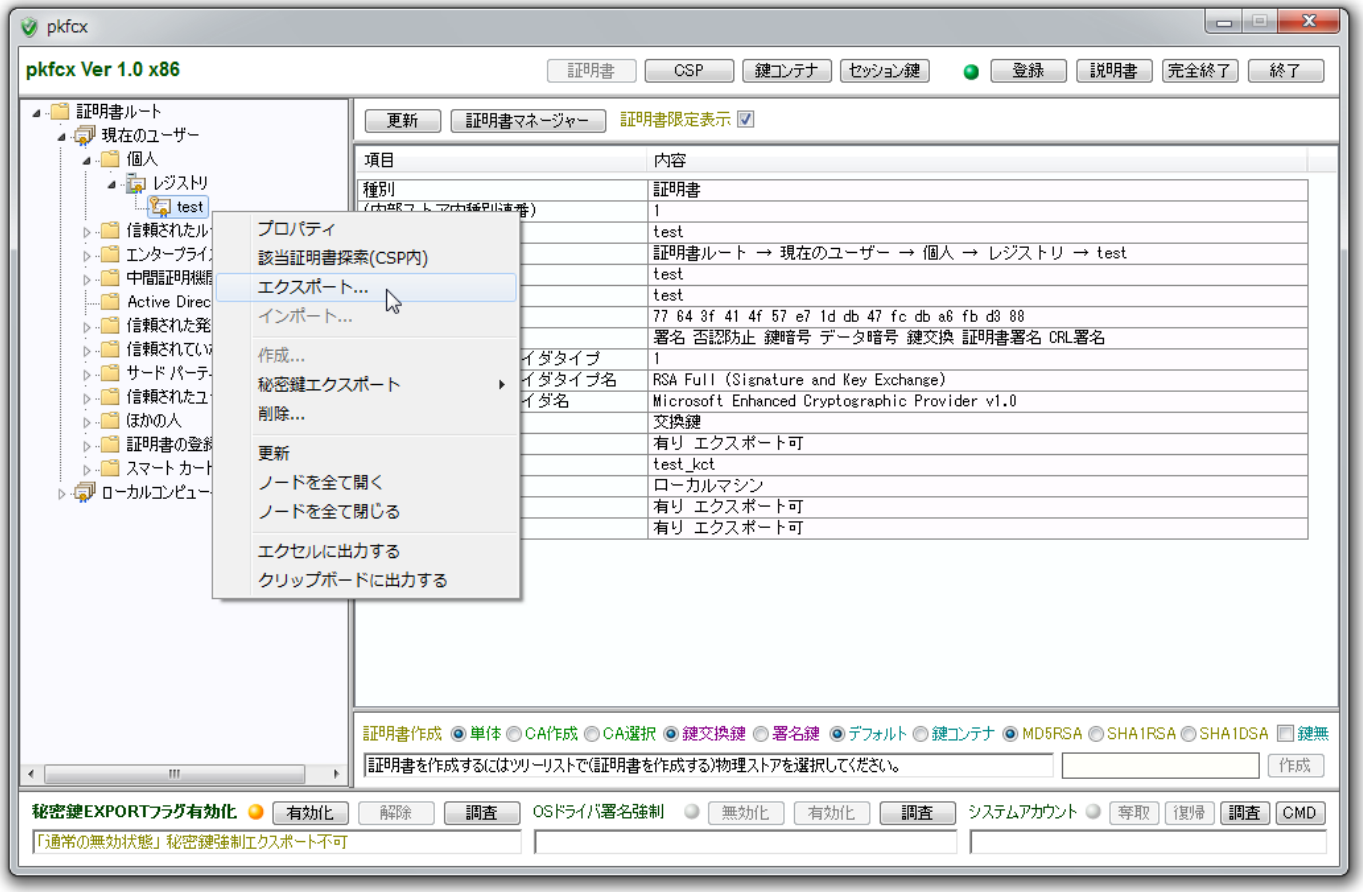


このように、また元の「エクスポート不可」な状態に戻ります。

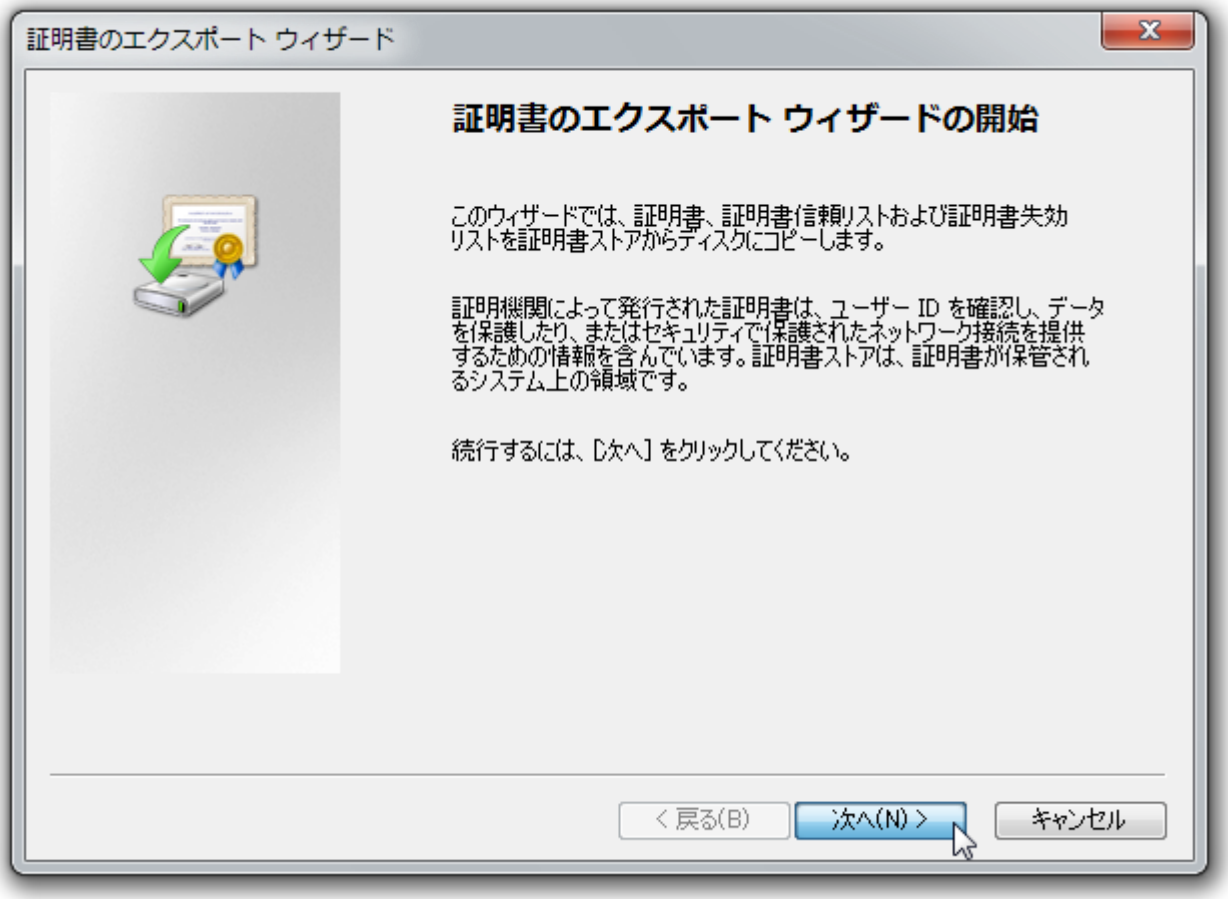


バックアップ（エクスポート）

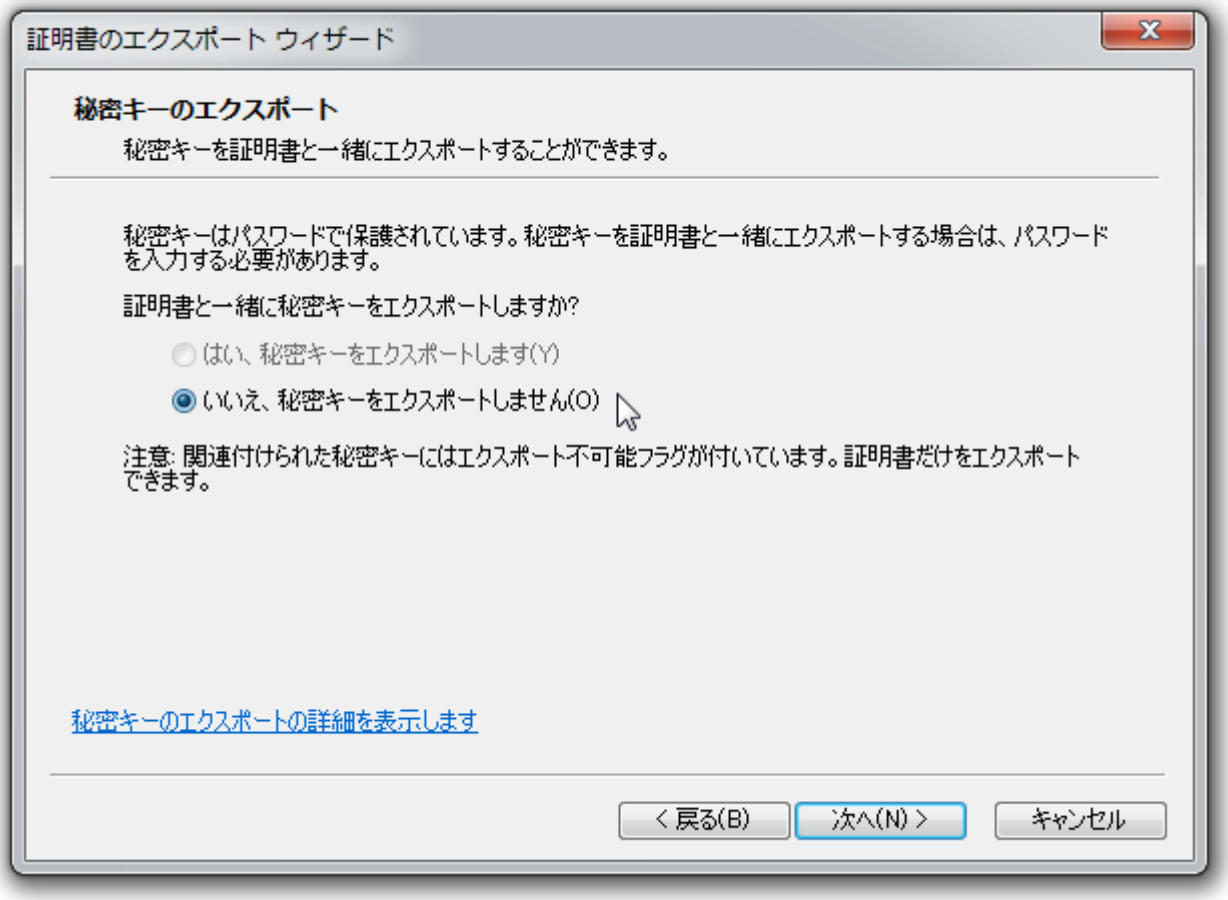
次に、<u>「証明書のエクスポート」すなわち「バックアップ」を行います</u>。「test」をエクスポート可能な状態にしてからコンテキストメニューを出し、以下のように「エクスポート」をクリックしてください。



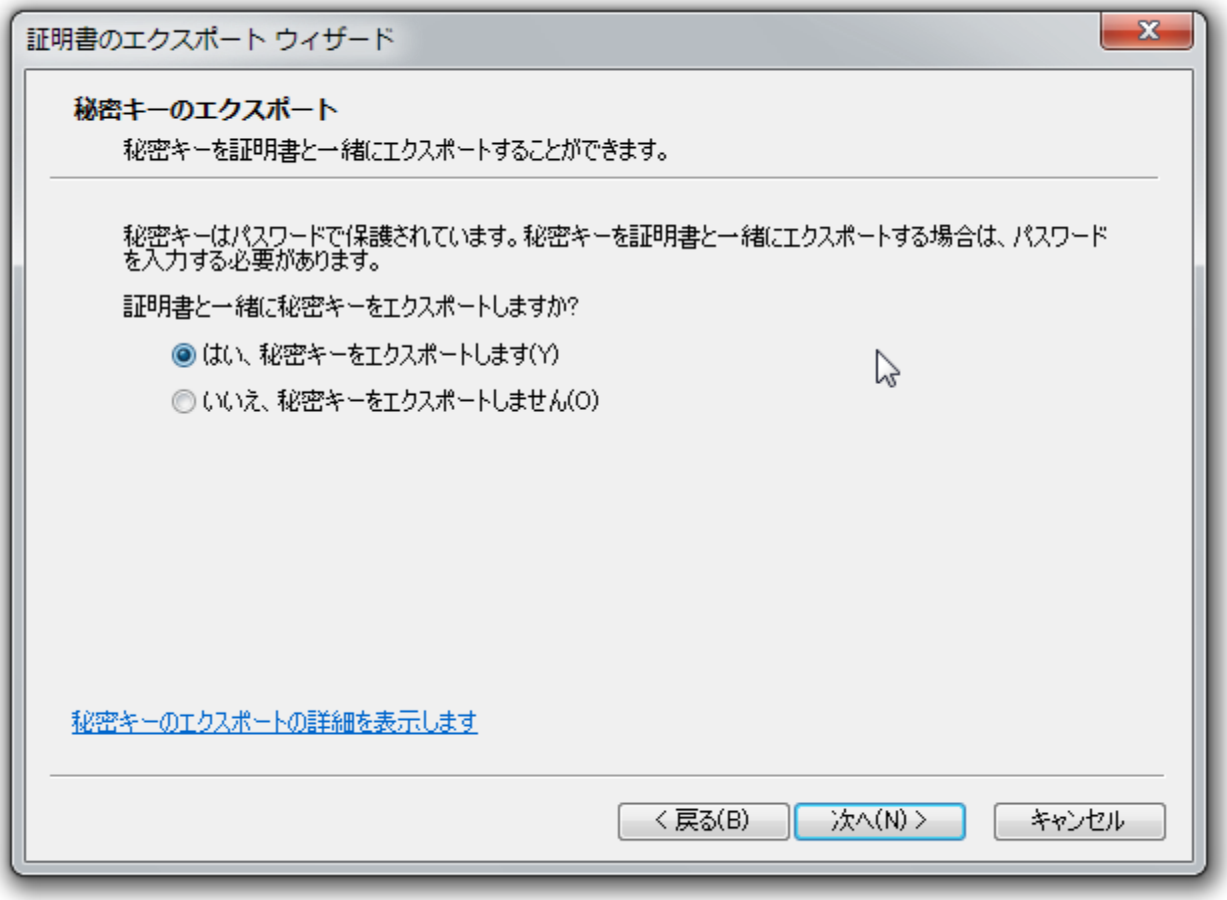
証明書のエクスポートウィザードが開始しますので「次へ」をクリックしてください。



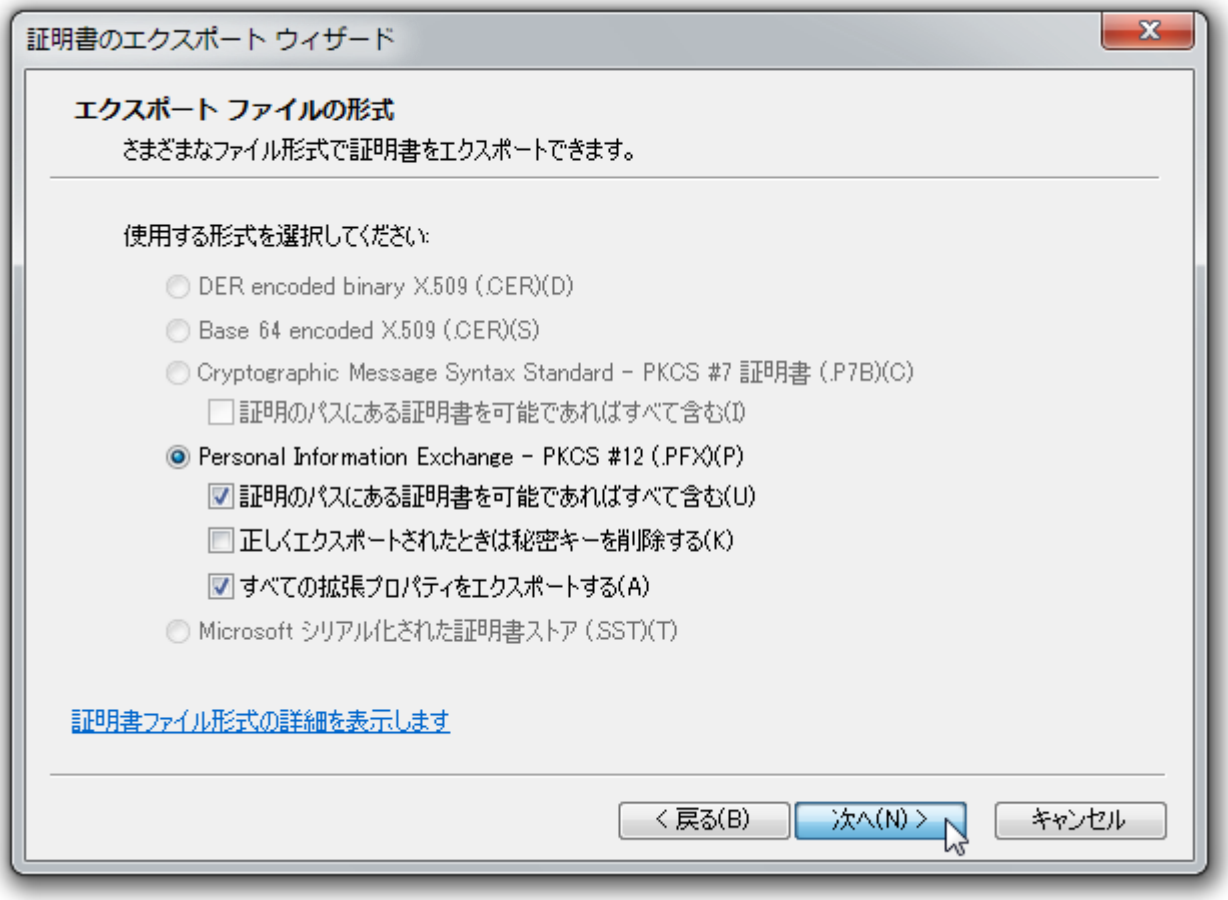
仮に「秘密鍵エクスポート不可」の状態ですと以下のような画面が出ますが、
ここでは既に「エクスポート可」に変更してありますのでこの画面は出ません。



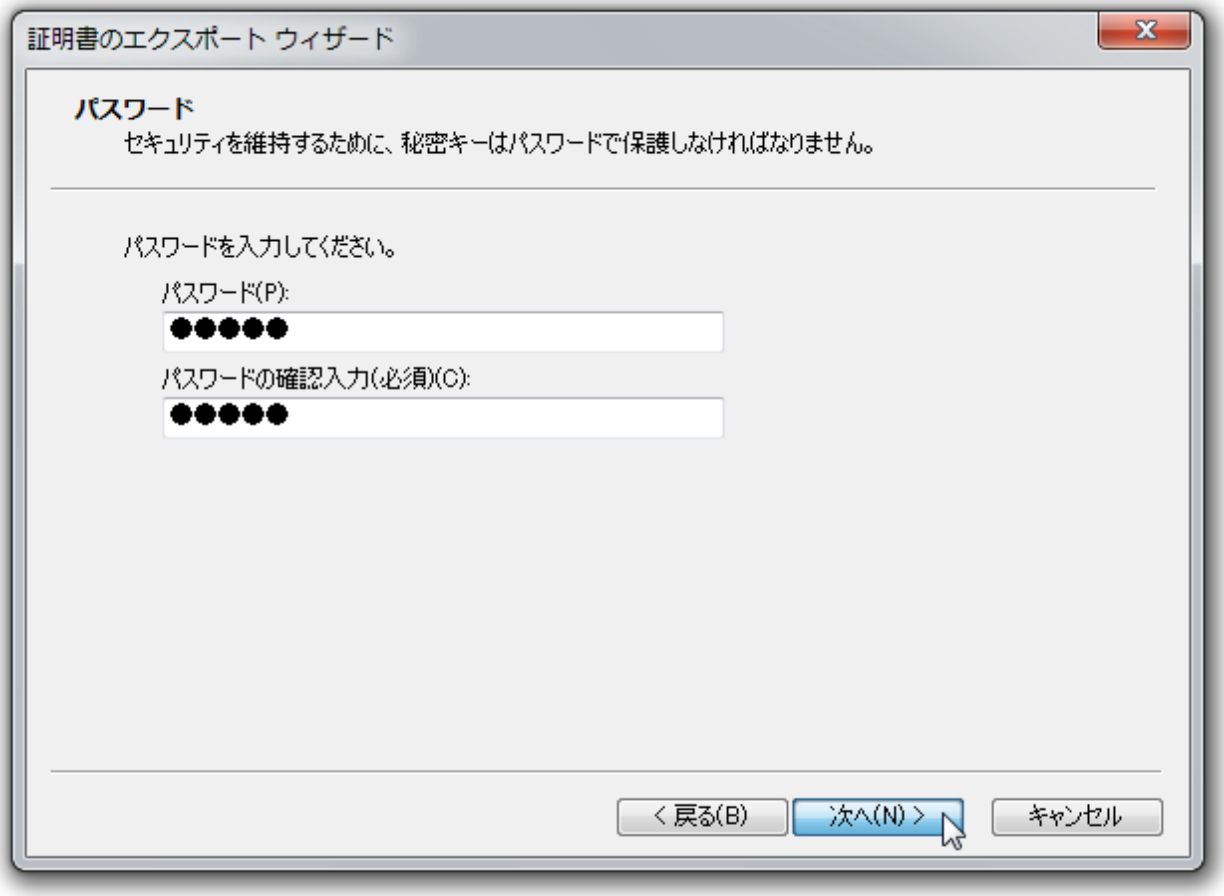
このような画面になります。「はい」の方を選択し「次へ」ボタンで進んでください。



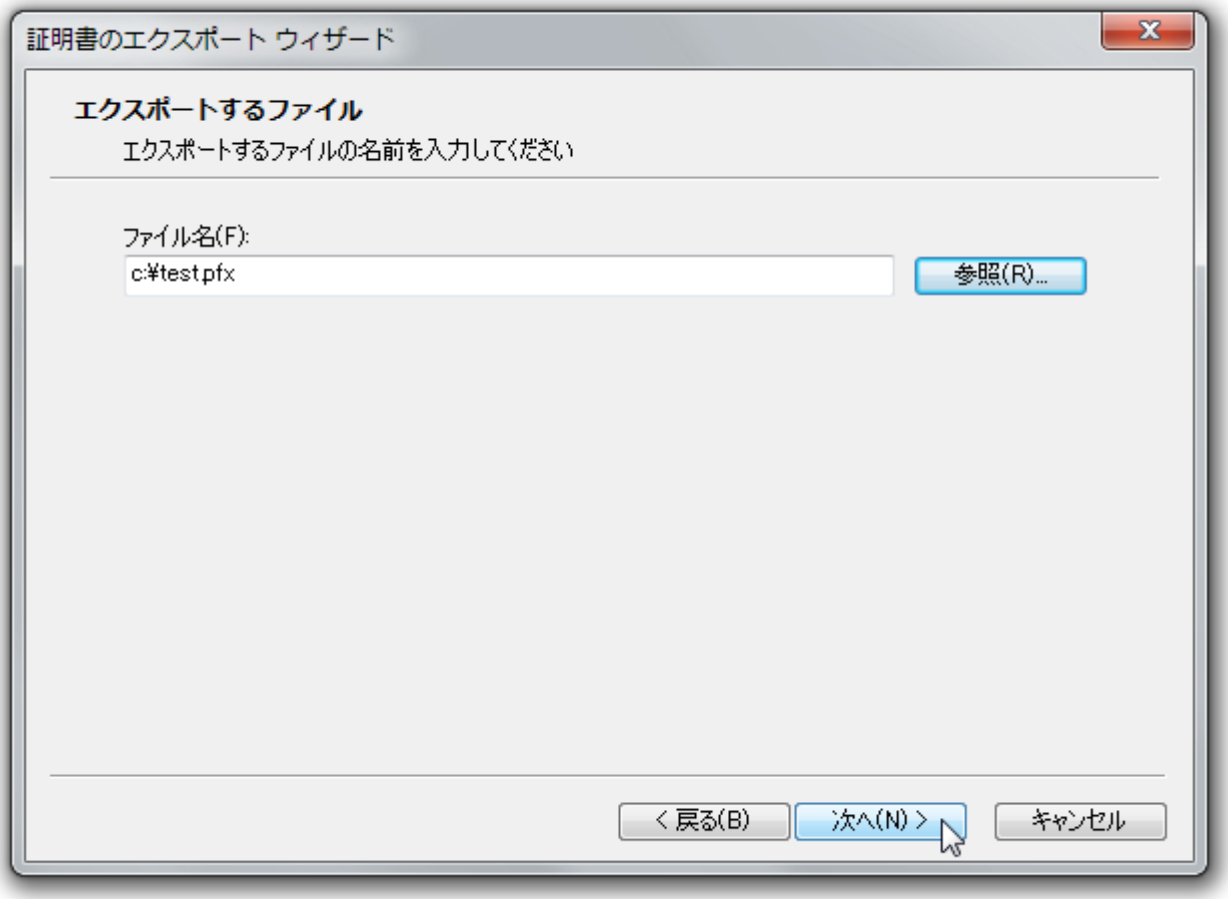
以下のように選択し「次へ」ボタンで進んでください。



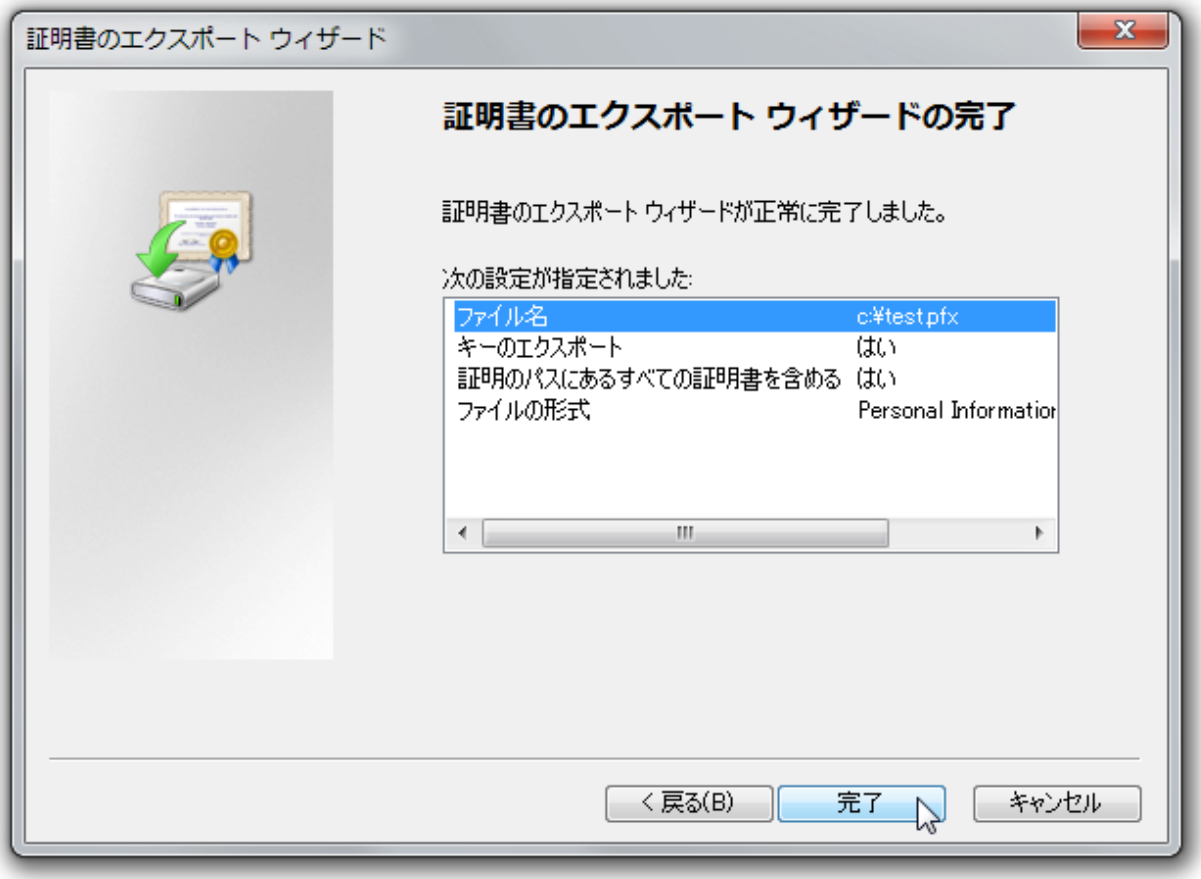
適宜に「パスワード」設定し「次へ」ボタンで進んでください。



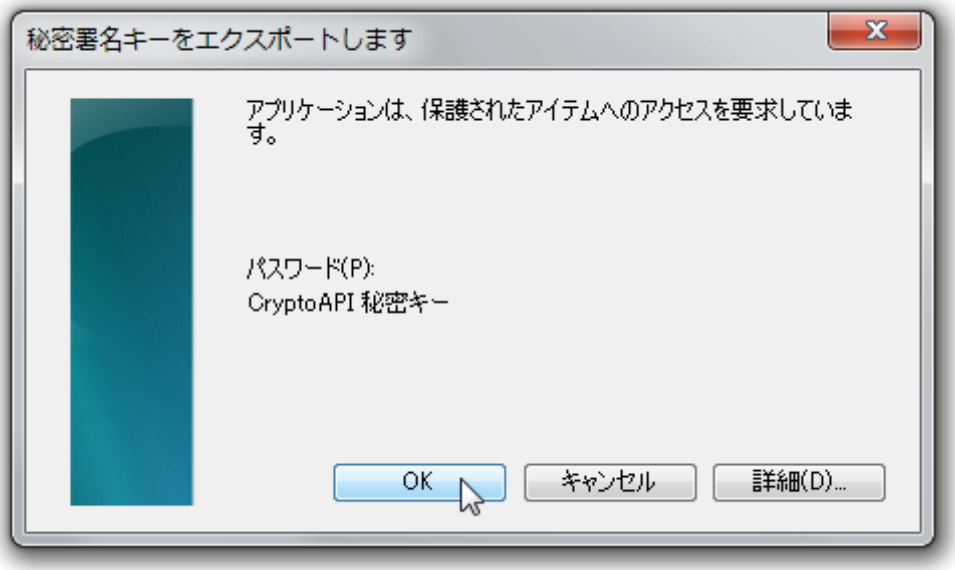
適宜に「エクスポートするファイル名」を設定し「次へ」ボタンで進んでください。

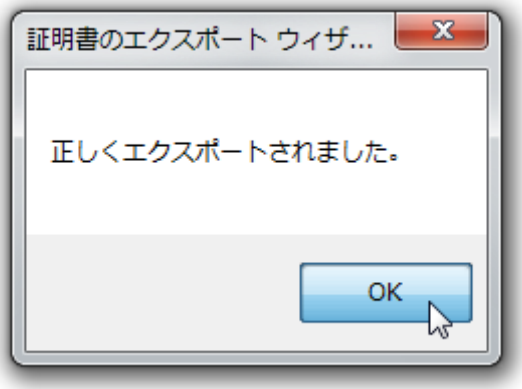


「完了」ボタンで進んでください。



このような画面が出たならば「OK」で進んでください。





これで「エクスポート」は完了です。

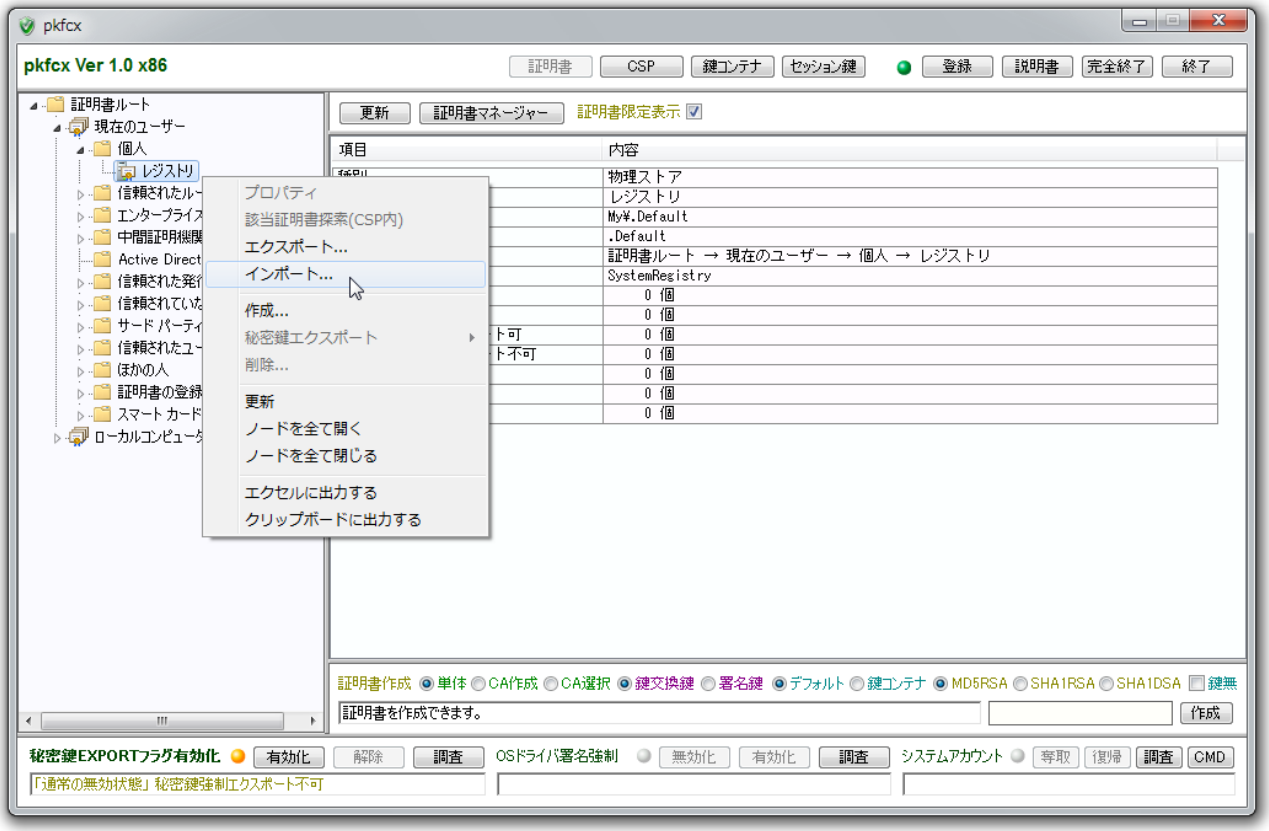
簡単「ネットバンキング電子証明書」リストア方法

ここでは先にバックアップした証明書のリストア方法を説明します。

リストア場所の選択

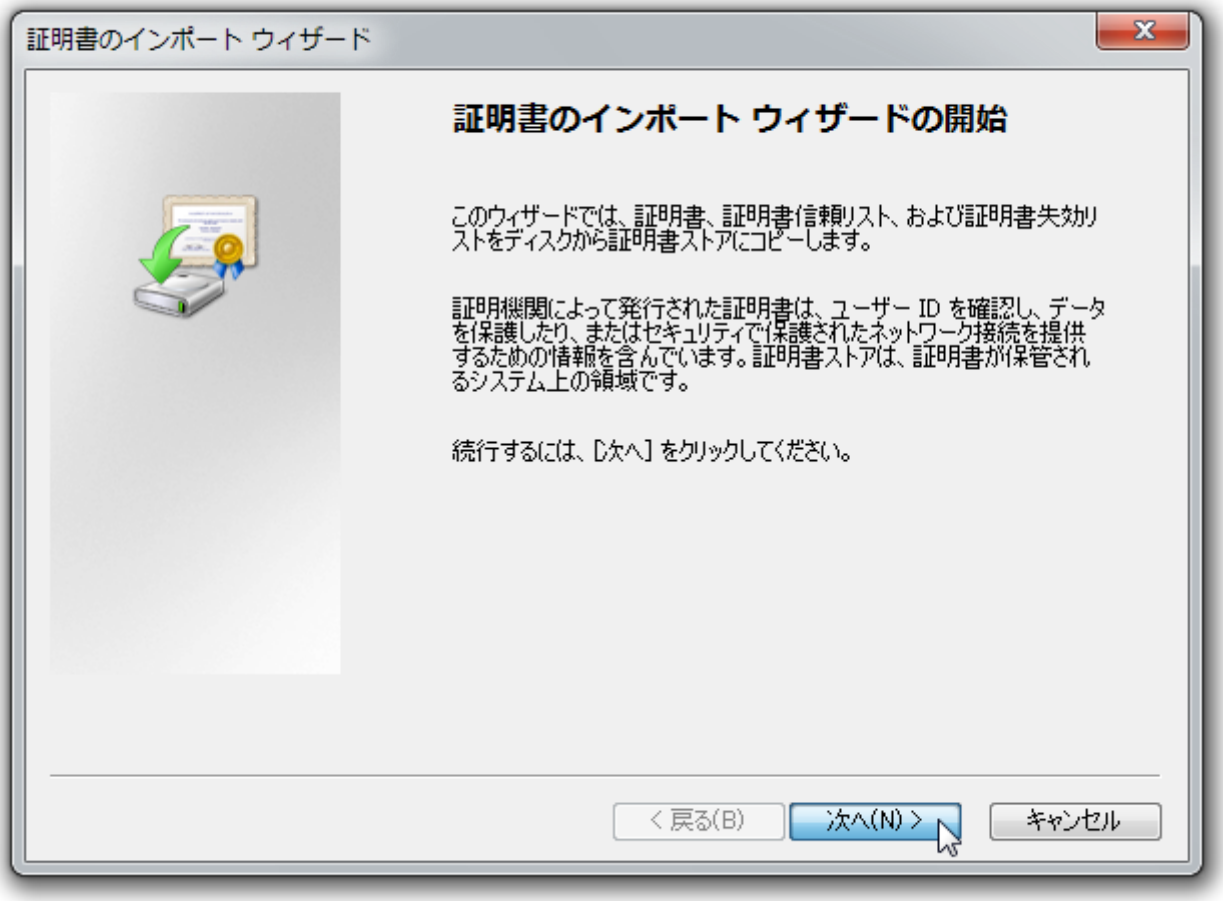
本ソフトを起動します。
バックアップの時と同様にツリーノードを展開し、証明書をリストアする物理ストアを選択します。

選択した物理ストア上でコンテキストメニューを出し「インポート」を選択クリックしてください。

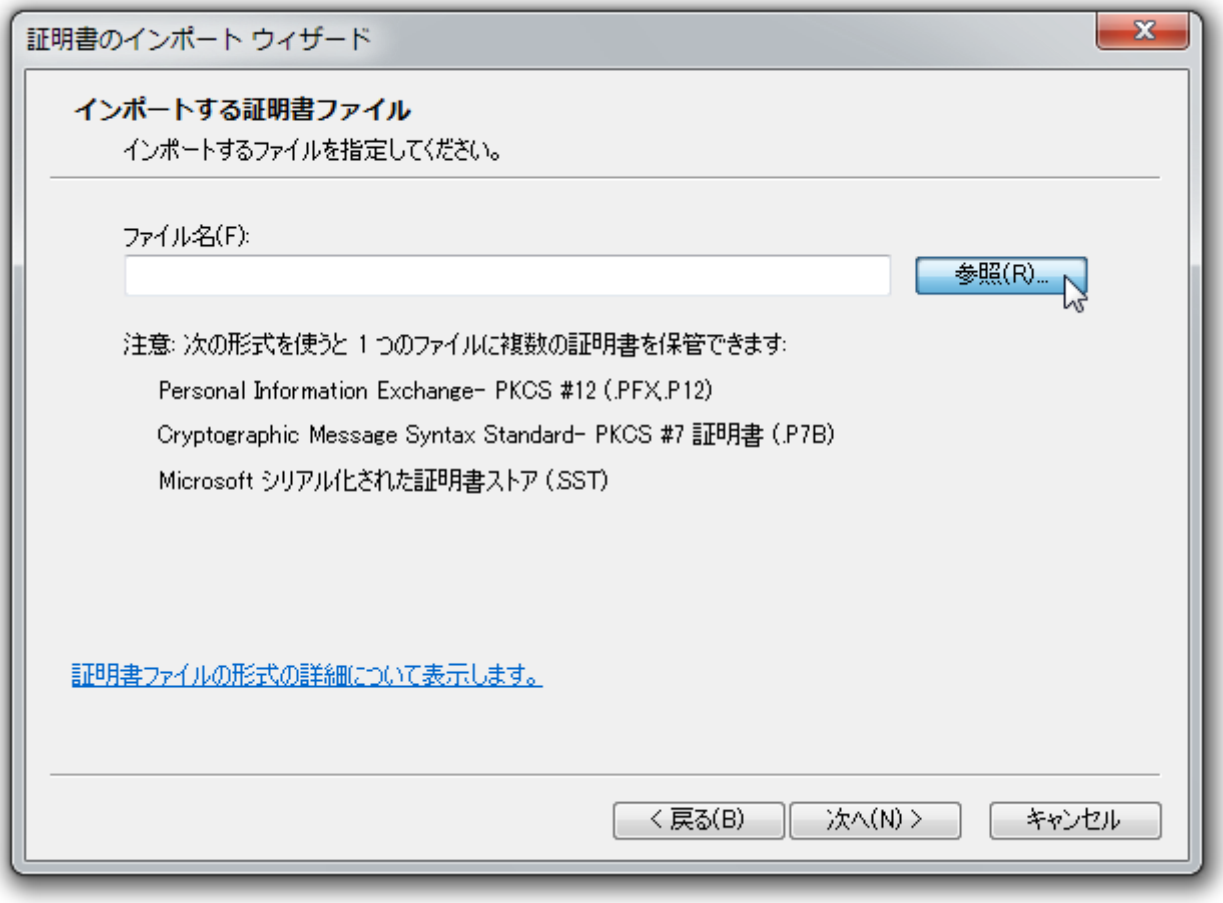


インポート

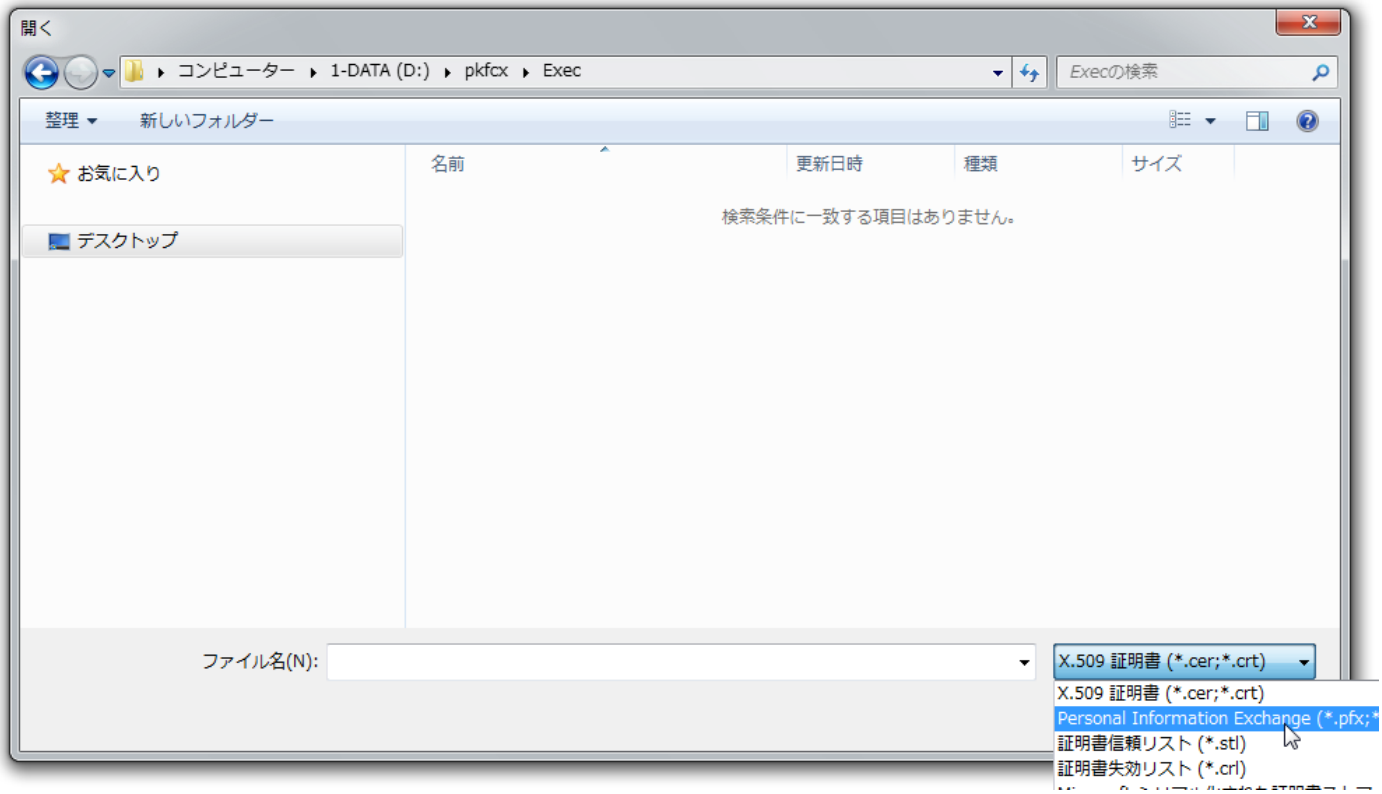
証明書のインポートウィザードが開始するので「次へ」で進みます。



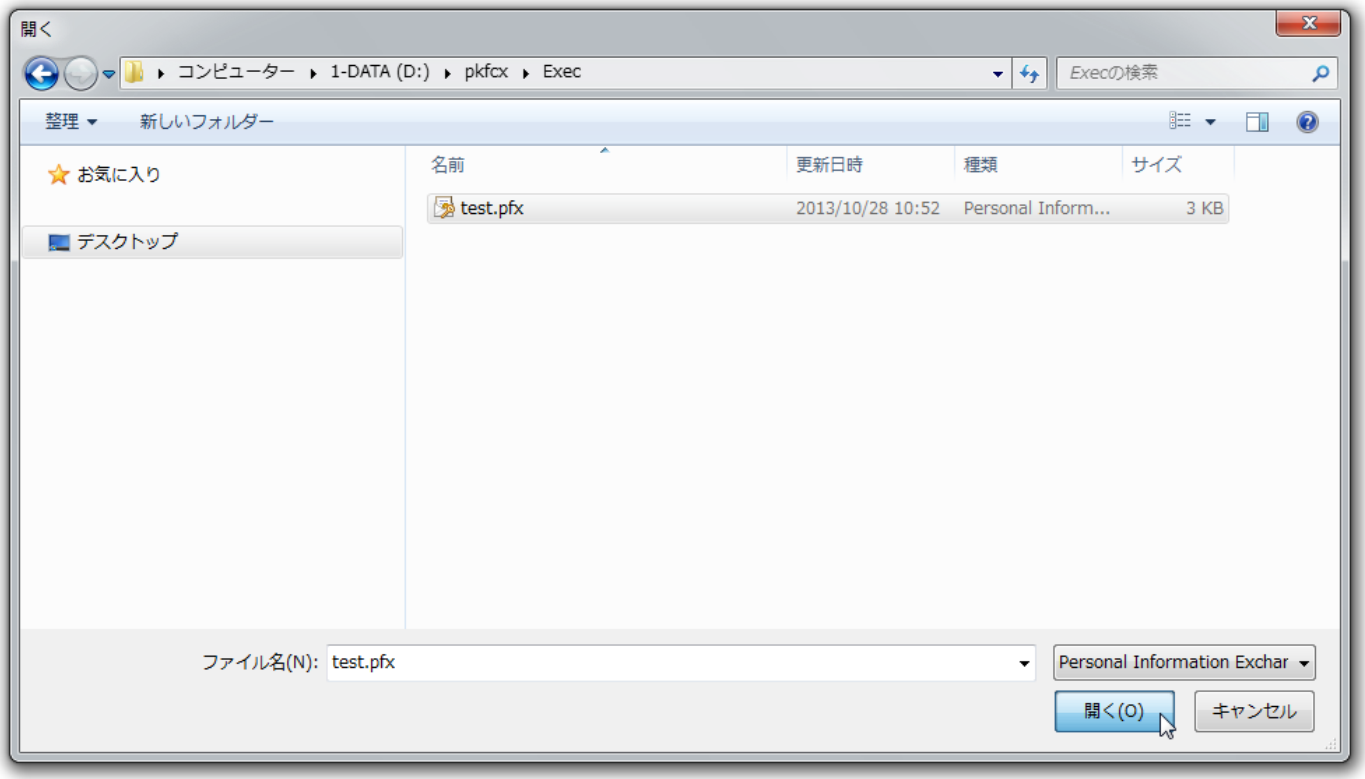
インポートするファイルの選択に入ります。「参照」ボタンを押してファイル選択します。



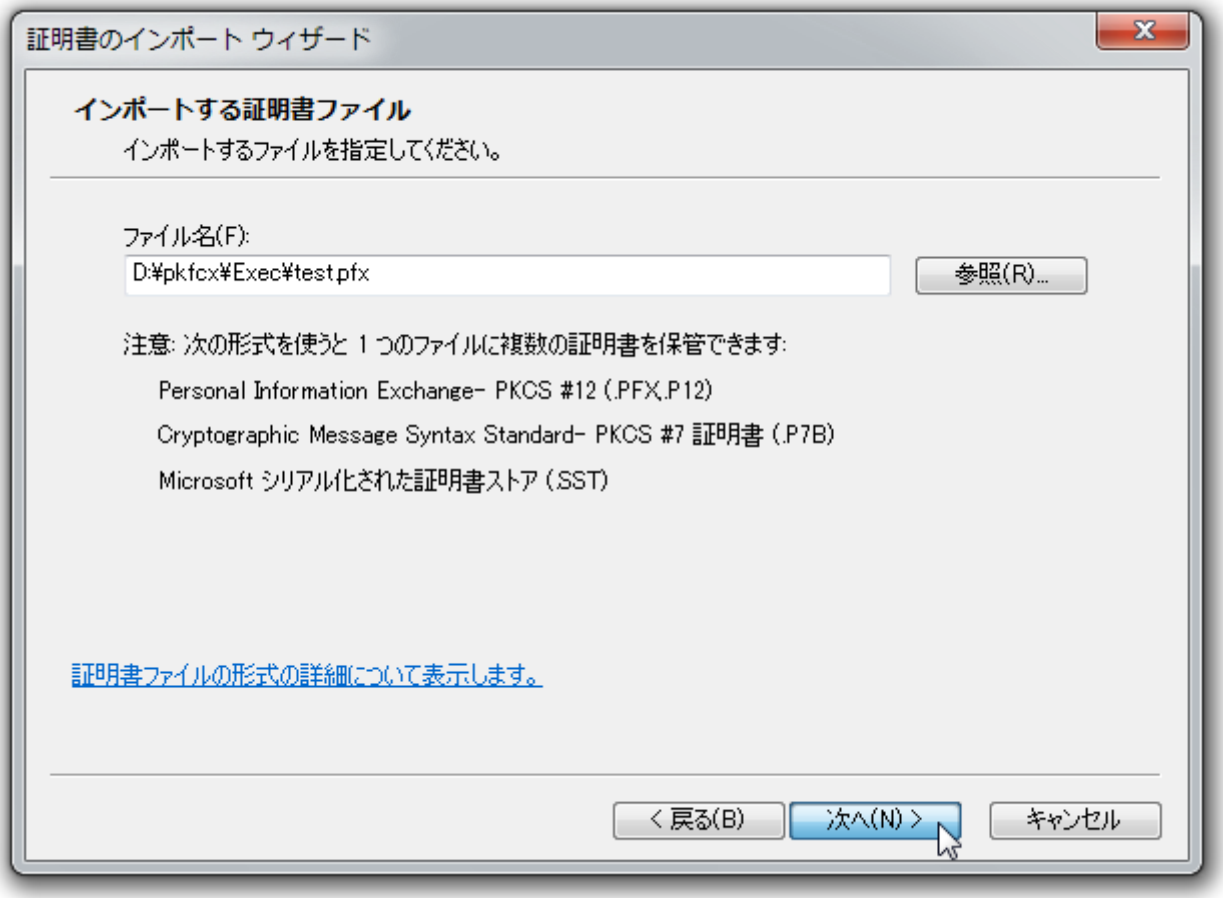
ここでは仮にインポートするファイル名を先ほどバックアップした「D:¥pkfcx¥Exec¥test.pfx」とします。
右下ファイル種別選択コンボボックスで「PersonalInformationExchange」を選択します。

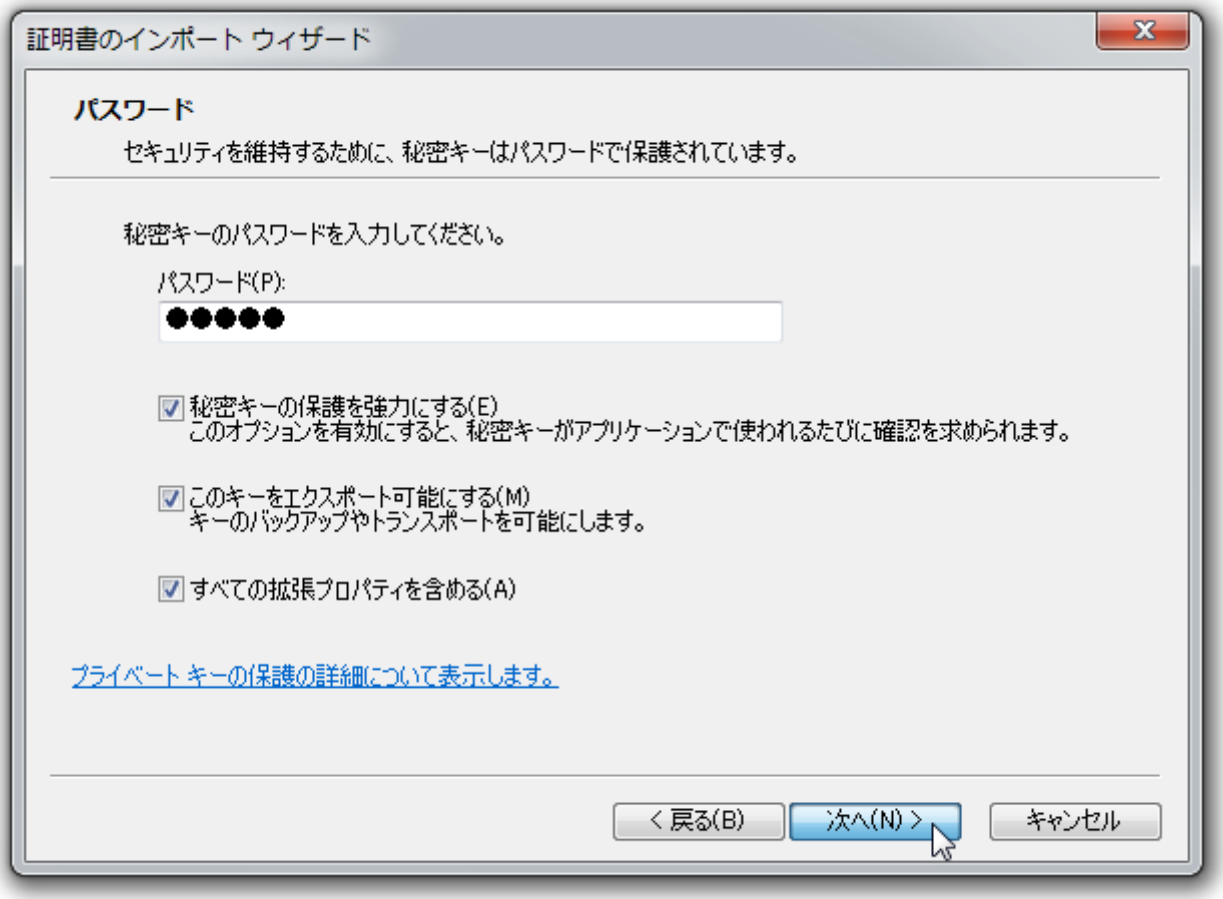


先ほどのバックアップファイルが表示されるのでこれを選択します。



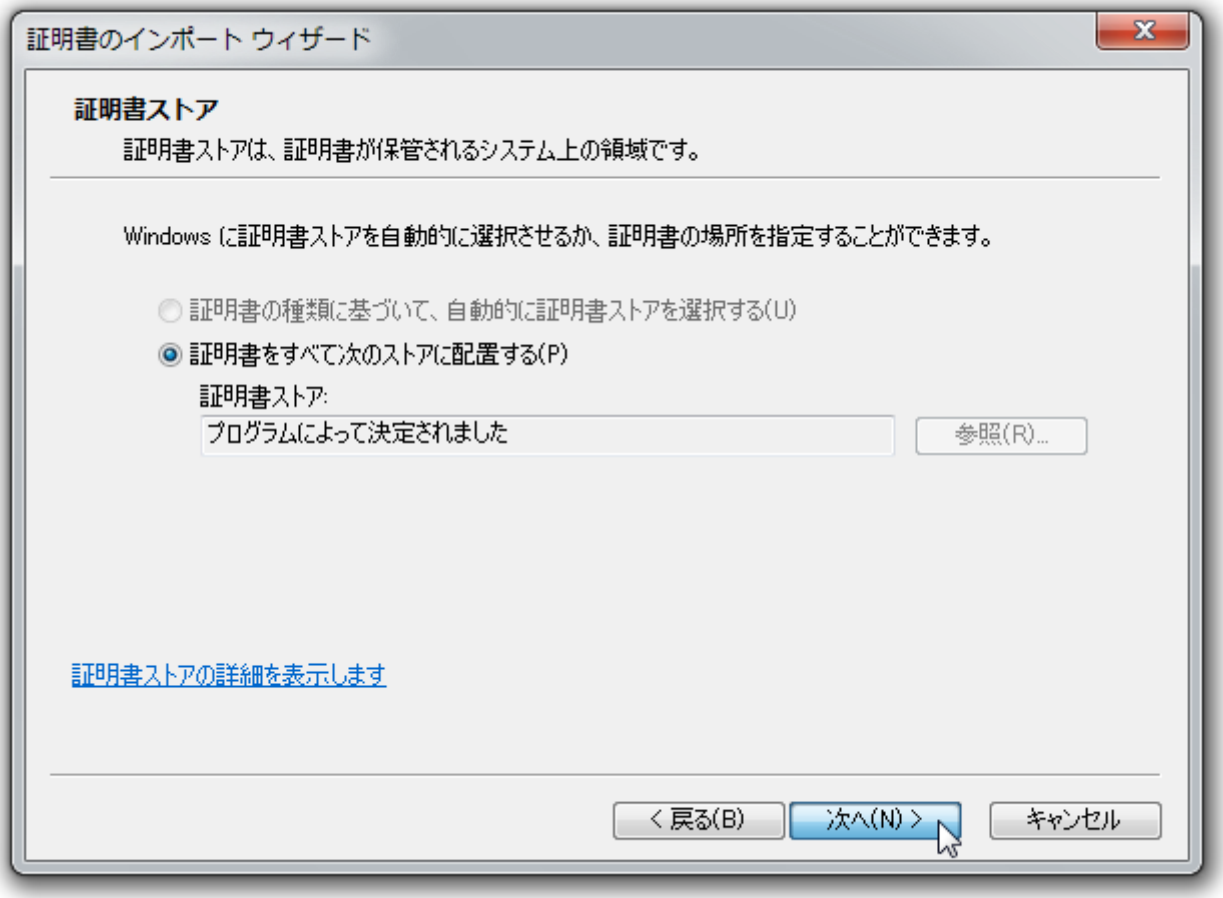
「次へ」で進みます。



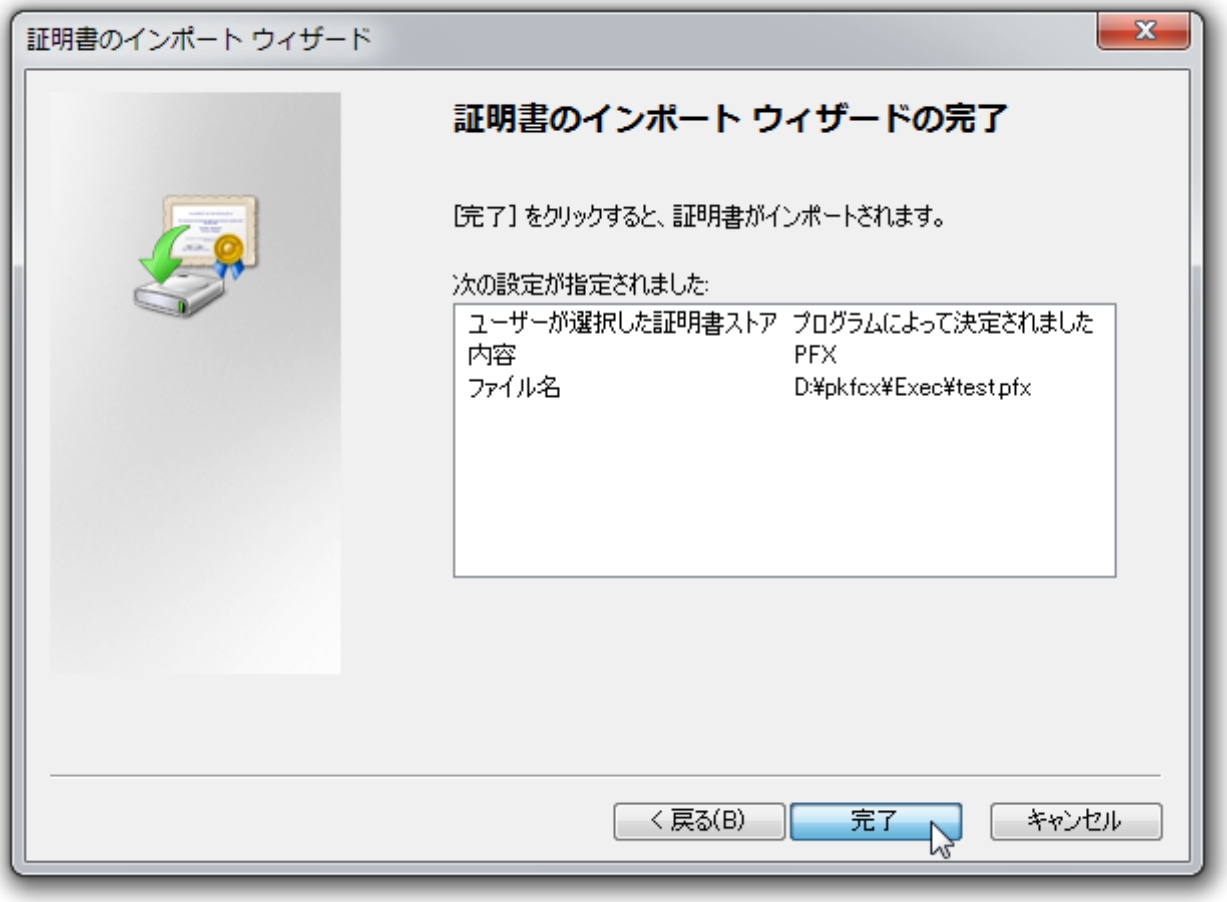


バックアップ時の「パスワード」を設定し、適宜オプションを設定して「次へ」進みます。
「秘密キーの保護を強力にする」これを設定すると鍵取扱局面で確認ダイアログが表示されるようになります。
「このキーをエクスポート可能にする」これを設定しないと「エクスポート不可」になってしまいます。
「すべての拡張プロパティを含める」一般的に設定してください。

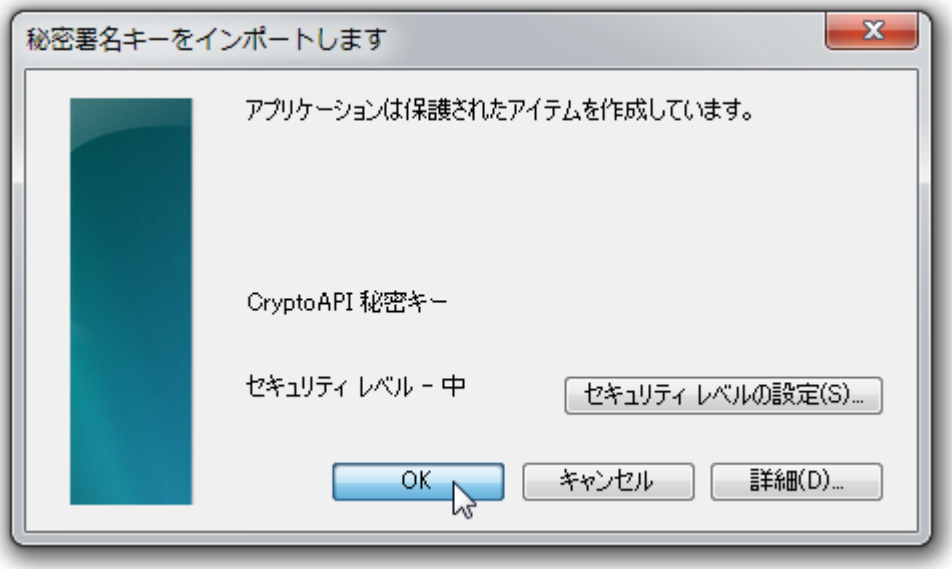
このような画面になるので「次へ」進みます。

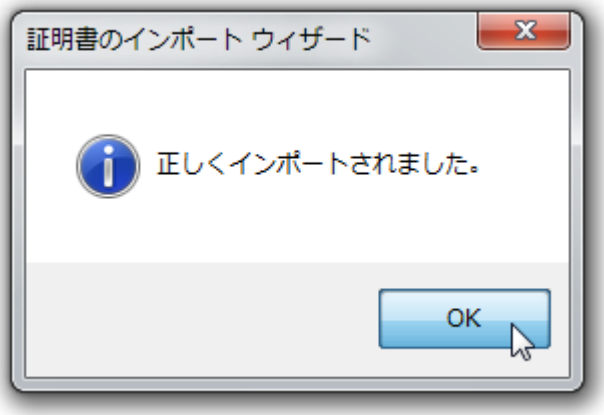


「完了」で進みます。



このような画面が表示されたら「OK」で進んでください。
場合によって(なんらかのプロセスでパスワード未設定のままこのシーケンスに入った場合)
「セキュリティレベルの設定」ボタンでこれに入りその設定を行わないと
「OK」ボタンが押せない場合もあります。





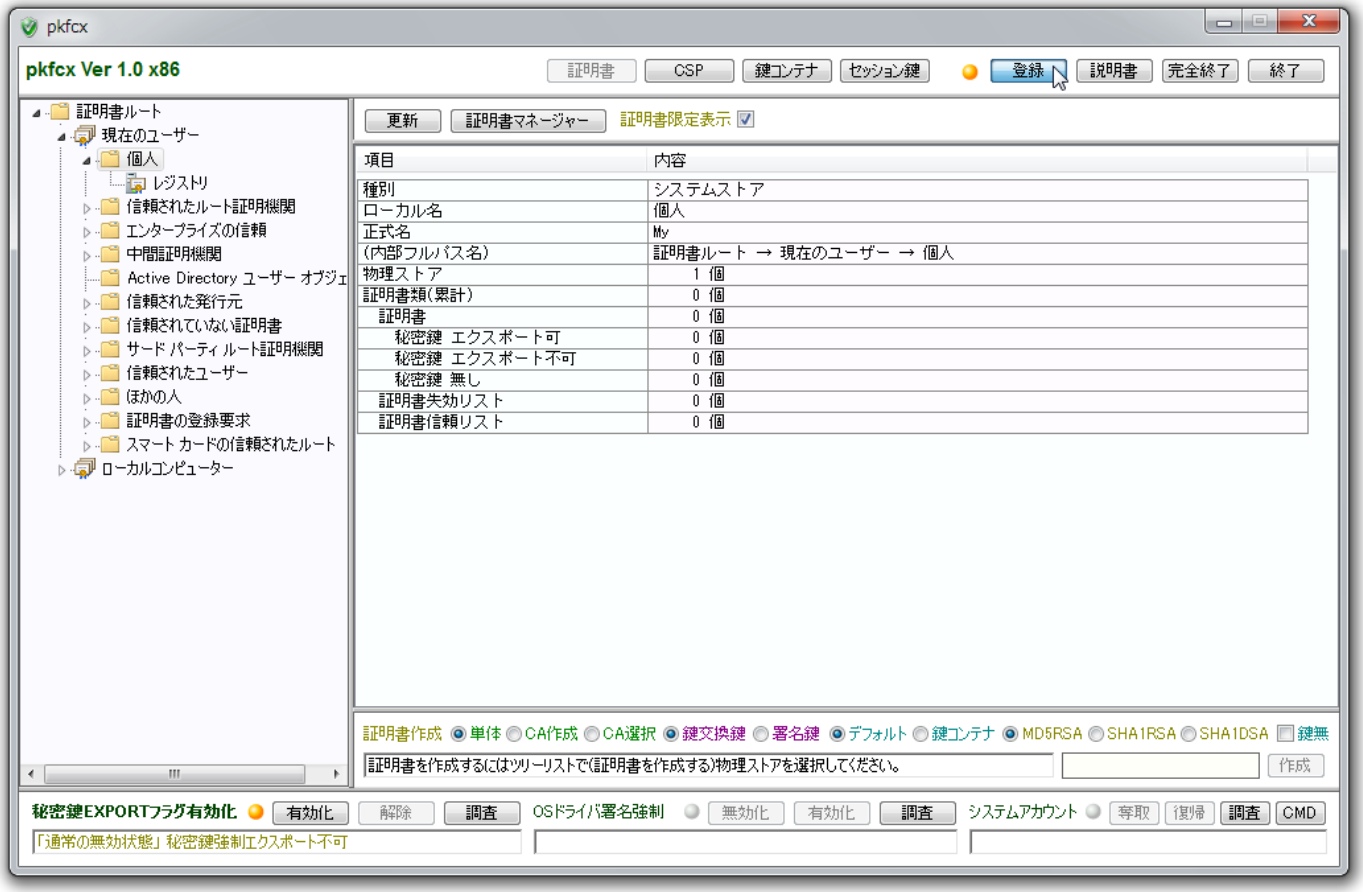
これで「インポート」は完了です。
ネットバンキング証明書の場合、この処理を別のパソコンで行うことでそのパソコンでもバンキング処理が可能になります。当然のことですが、証明書をバックアップしたファイルは、その別のパソコンで USB メモリ等を経由して読めるようにしておく必要があります。

証明書チェーンについて

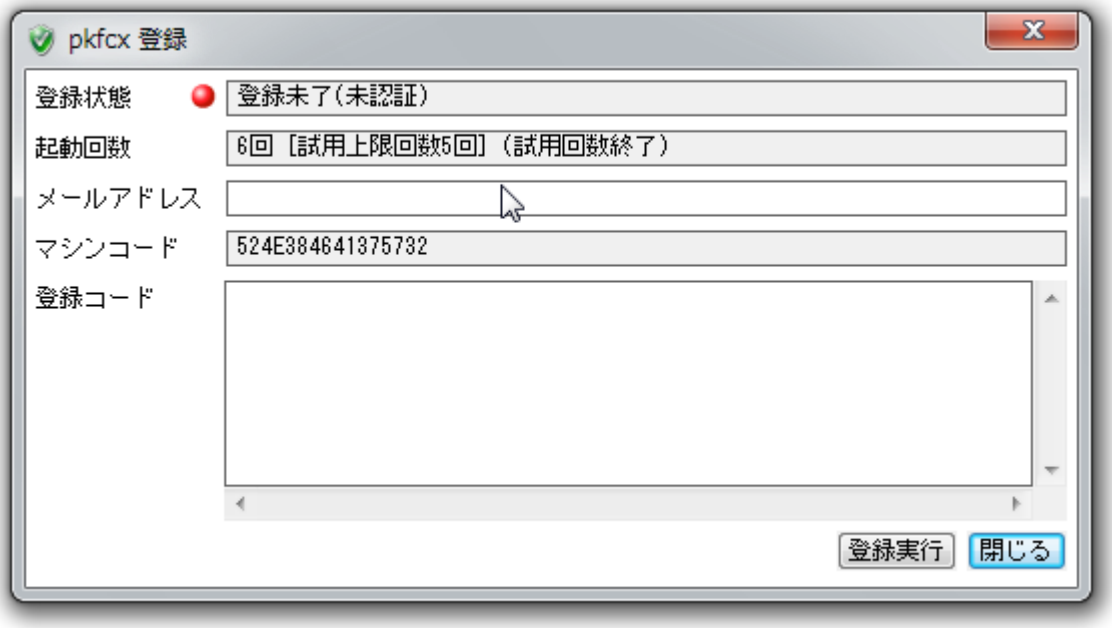
原則、ターゲットの証明書を認証した CA 証明書関係の証明書チェーンもこれで復旧されますが、
場合によって復旧されないこともあります。
但し、この証明書チェーンが崩れていてもバンキング処理自体(ログインや取引)はできます。
あえてこの崩れた証明書チェーンを完全に復旧するには、
適宜ターゲット証明書の CA 証明書を手に入れ、
適宜なストア(信頼されたルート証明機関)にこれを入れる必要があります。
金融機関によって CA 証明書を公開しているところもありますが、
多くの場合これは公開されていないので、
これを入手するには元のパソコンからこれを見つけ、
適宜これをエクスポート・インポートする必要があります。

(購入)登録(認証)方法

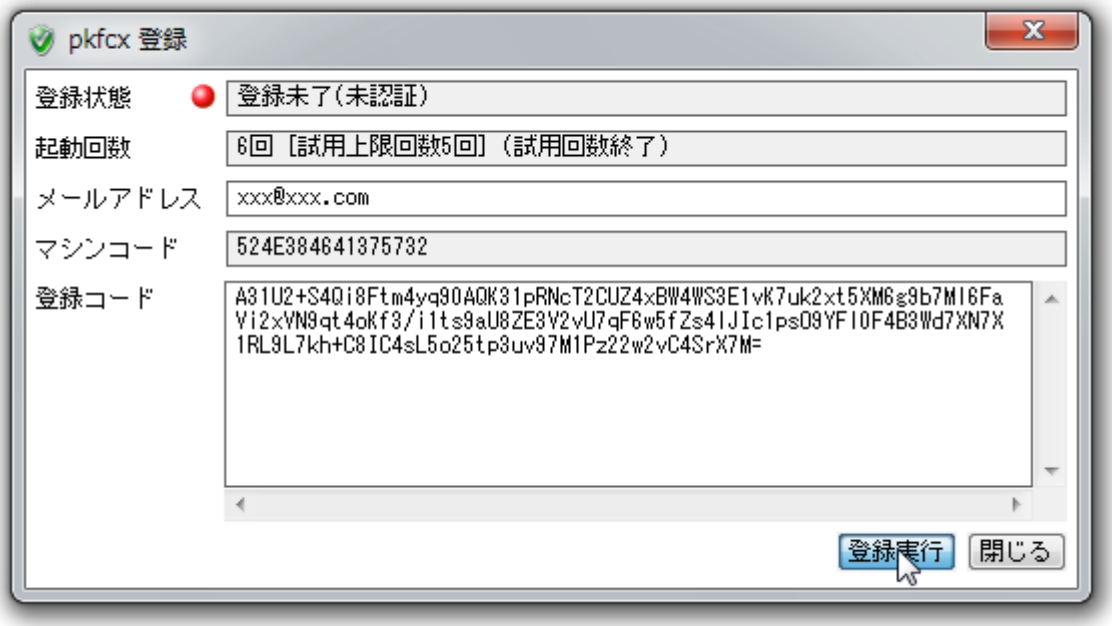
試用制限解除の(購入)登録(認証)方法を説明します。
「登録」ボタンを押してください。



このような画面が表示されます。
赤いマークが出ていますがこれは試用回数超過で未認証を示します。
試用回数未満で未認証のときは黄色、
認証状態では緑色になります。
ここで「マシンコード」は無関係なので無視してください。



登録申請したときの「メールアドレス」と取得した「登録コード」を(コピペで)入力して
「登録実行」ボタンを押してください。
登録コード内で右クリックすると
「ペースト」等の機能リストが表示されるのでそれを使って入力してください。



正しい登録コードを入力し「登録実行」ボタンを押すと「認証完了」します。
以下のようになれば「登録完了」です。「閉じる」で登録シーケンスを終了します。

起動回数のカウントは本ソフトを何回起動したかどうかで、
証明書のエクスポートアクション数とは無関係です。
試用中はなるべく起動した本ソフトを終了せずに、
連続して証明書が正しくエクスポートできるか検証してください。

「pkfcx-mini」での登録

「pkfcx-mini」でも別途キー登録が必要です。送付された「pkfcx-mini」用の登録コードを登録してください。
操作は「pkfcx」と同様なので上記を参照してください。

「pkfcx-mini」でのバックアップ方法

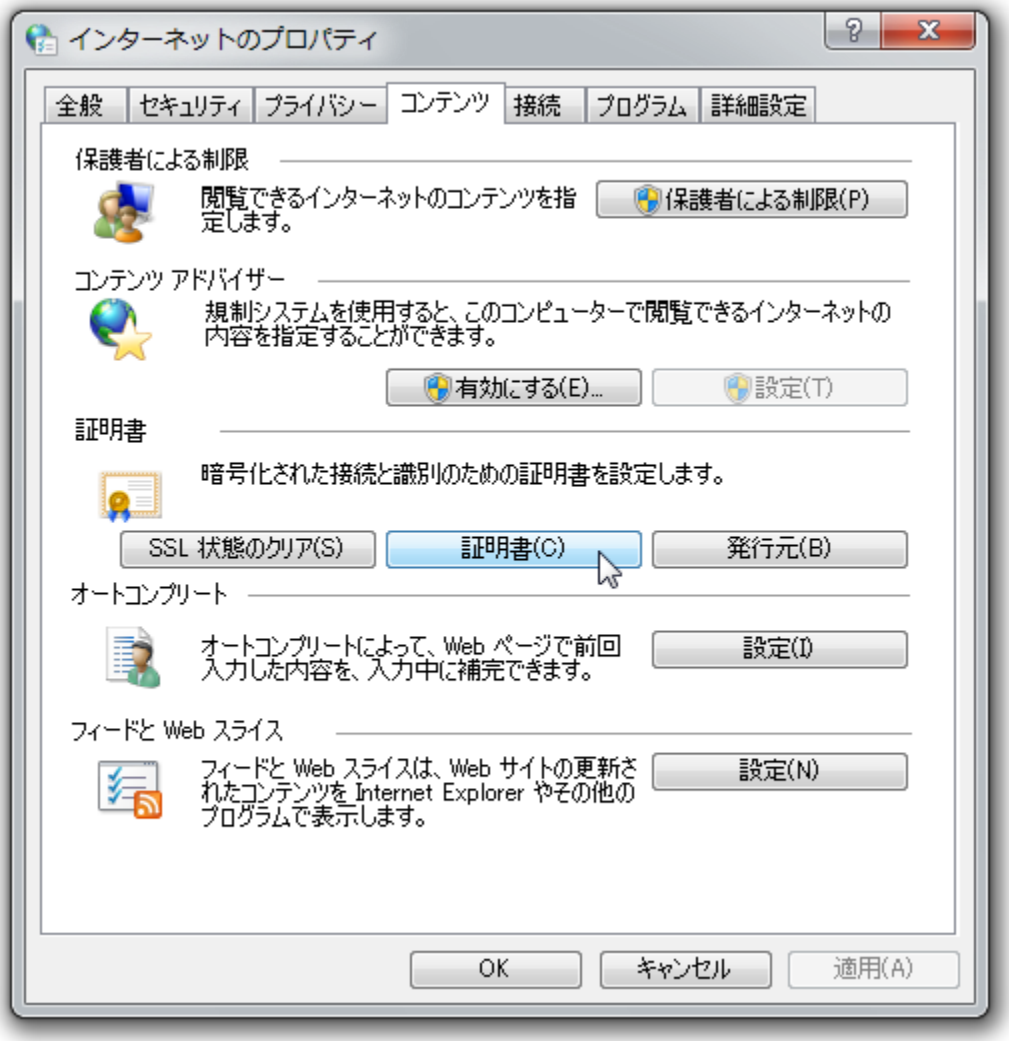
ここでは仮に Windows7-SP1 x86 環境の例で説明します（他の環境では多少の違いがありますが同様です）。

ターゲット証明書の選択

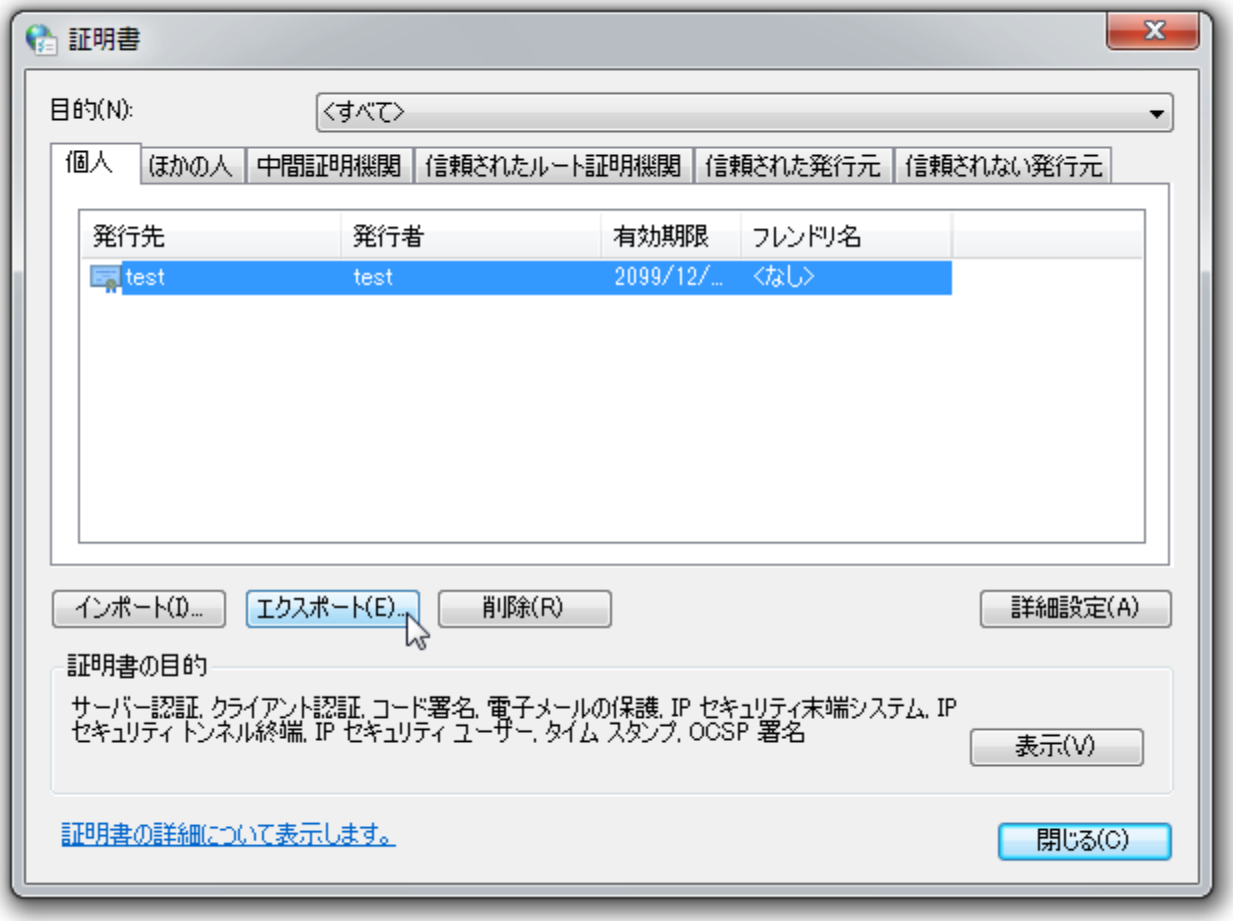
「pkfcx-mini」を起動します。
OS 起動後の本ソフト「初回起動時」は本ソフトによるシステム「調査」に時間が掛るため数秒から十数秒待機してください。画面左下にその旨表示されます。2 回目以降は待たされることはありません。
尚「pkfcx_mini」は「pkfcx」と同時には起動できません。

調査が終了すると以上のような画面が現れます。まずは「証明書」ボタンを押してください。

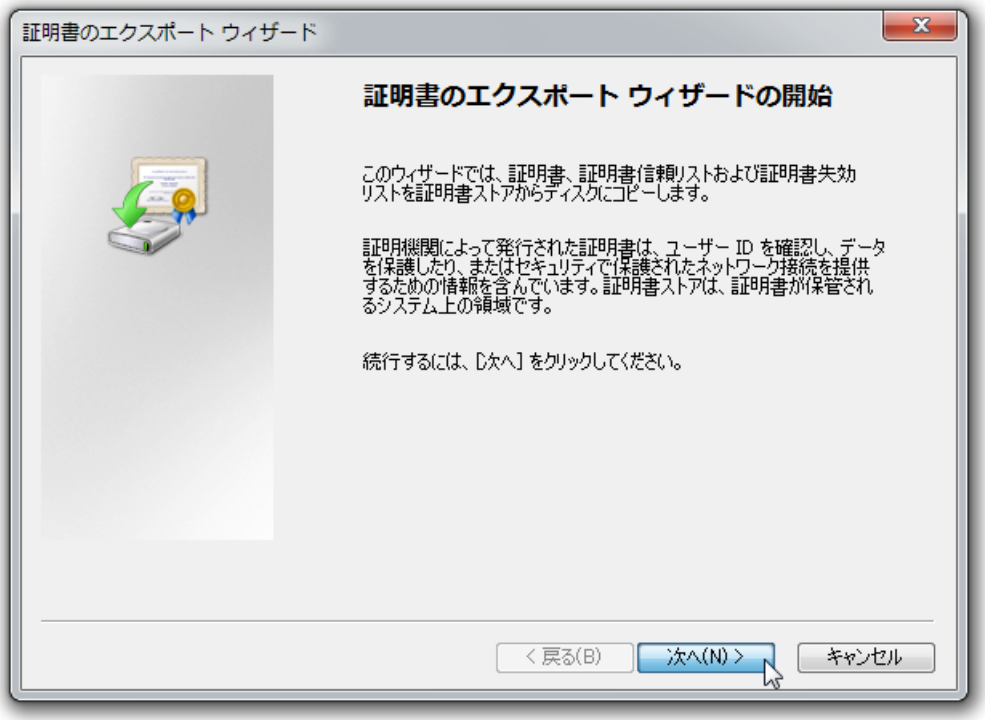
以下のような画面が現れるので「証明書」ボタンを押してください。



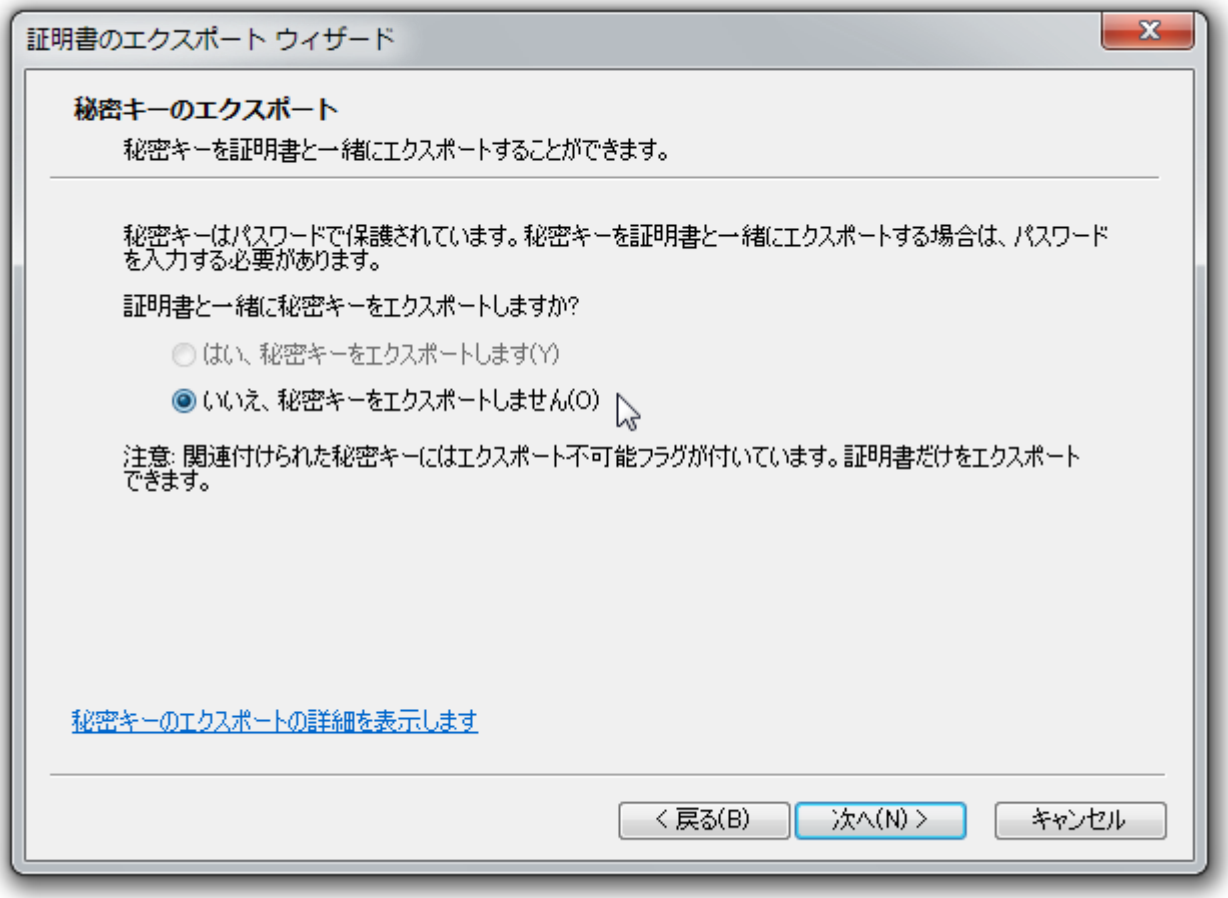
以下のような画面になり「証明書」が列挙されます。例として「test」という名前の証明書が見えています。
ここでターゲットとなるネットバンキング用の電子証明書を選択してもらうことになりますが、
以降、説明のため「test」がターゲットとなる証明書と仮定して話を進めます。
ターゲットとなる証明書がわからない場合、通例その名前に関連する文字(金融機関名等)が入っていますのでそれを頼りに見つけてください。この説明では「個人」にターゲット証明書があると仮定していますが、かならずしもそこにターゲットがあるとは限りませんので、みつからない場合は別の場所も探してください。
尚、この「test」という証明書は、一般的なネットバンキング用電子証明書と同様に「秘密鍵エクスポート不可」になっていると仮定して話を進めます。図のように「test」を選択し「エクスポート」ボタンを押してください。



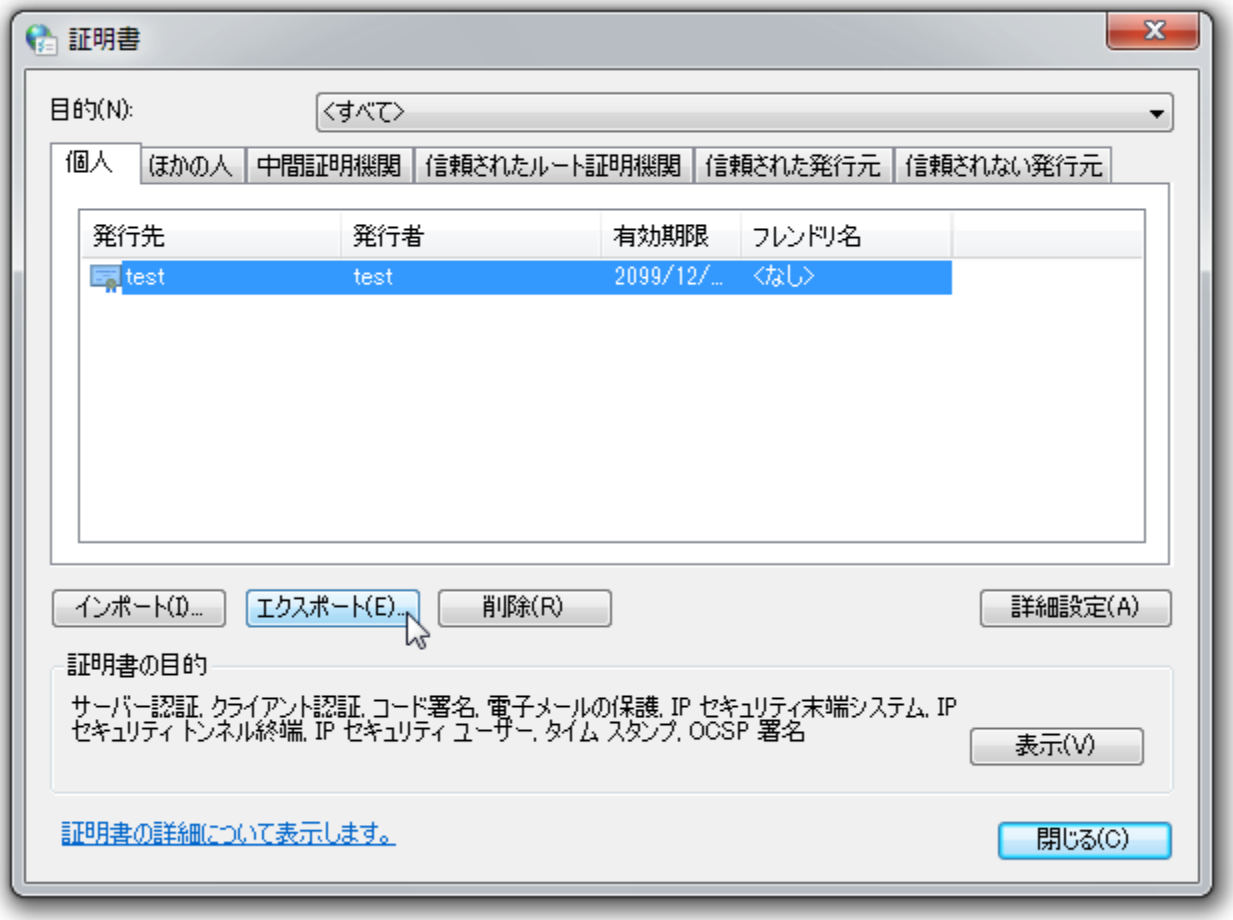
証明書のエクスポートウィザードが開始しますので「次へ」をクリックしてください。



「秘密鍵エクスポート不可」の状態ですと以下のような画面が出て、完全なバックアップがとれません。



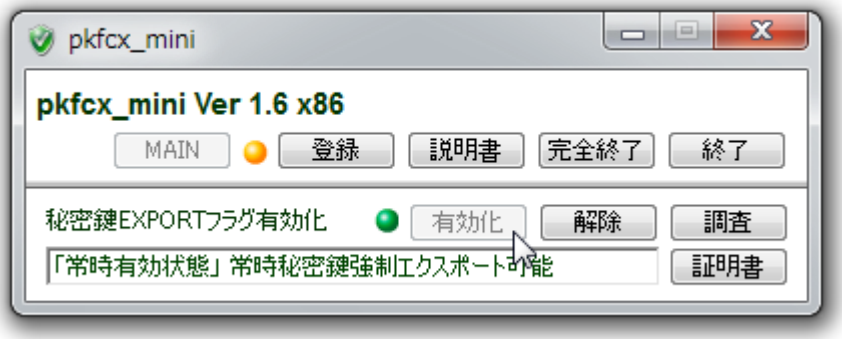
ここで「キャンセル」ボタンを押して上の画面を閉じてください。
下の画面に戻ります。この画面はそのままで、本ソフトの画面に戻ってください。



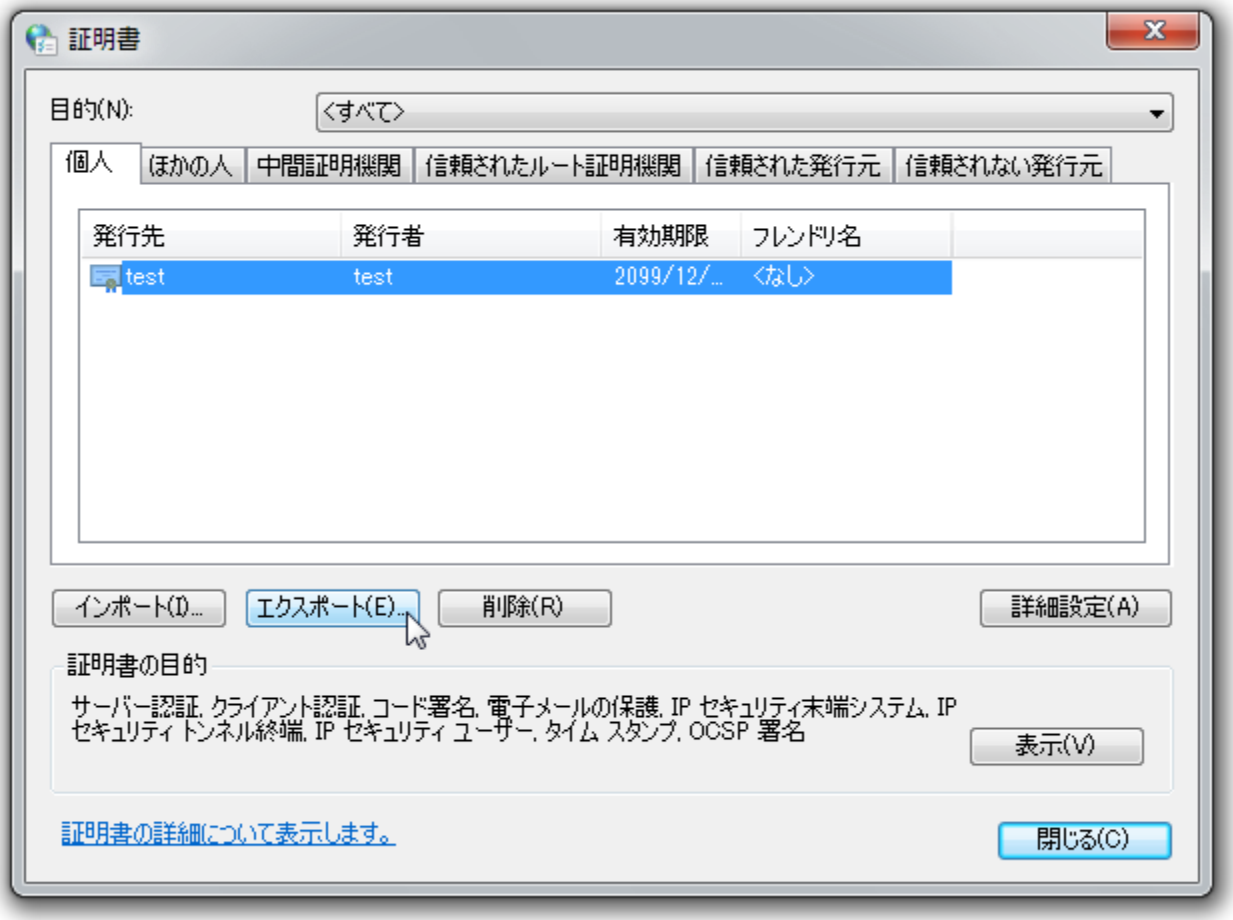
エクスポート可能化

次に、秘密鍵エクスポート不可状態を解除してエクスポート可能化します。
本ソフトの「有効化」ボタンを押してください。

下のような画面になります。

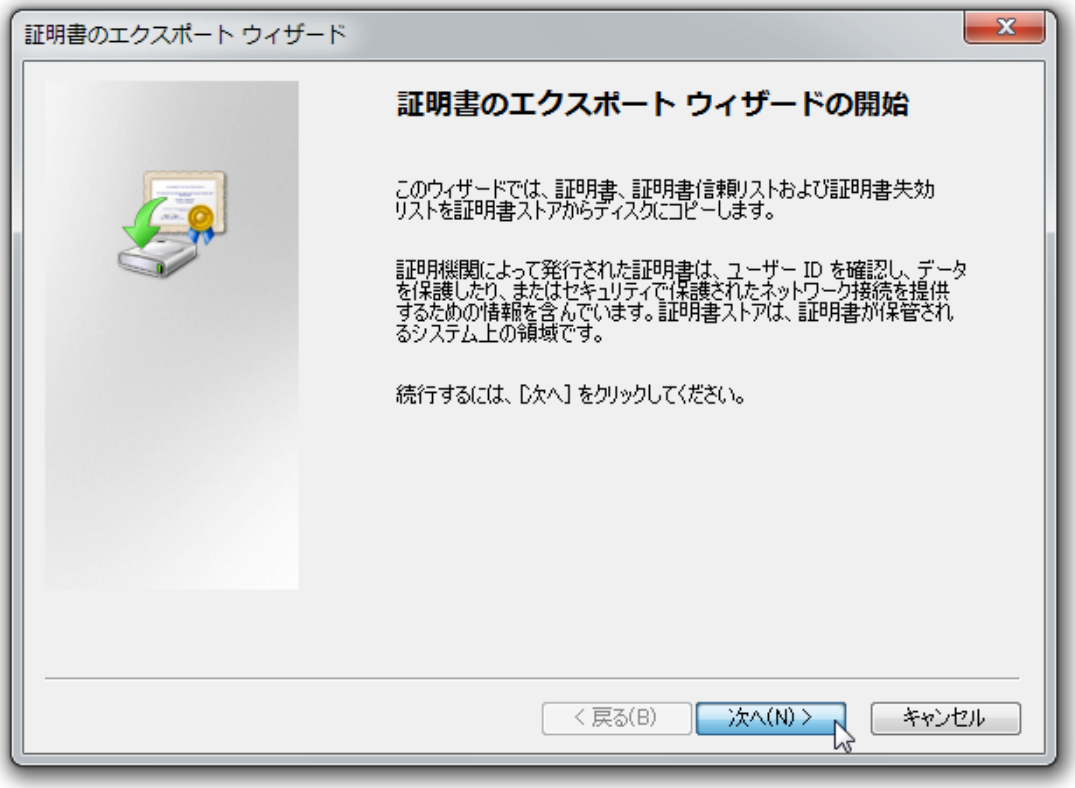


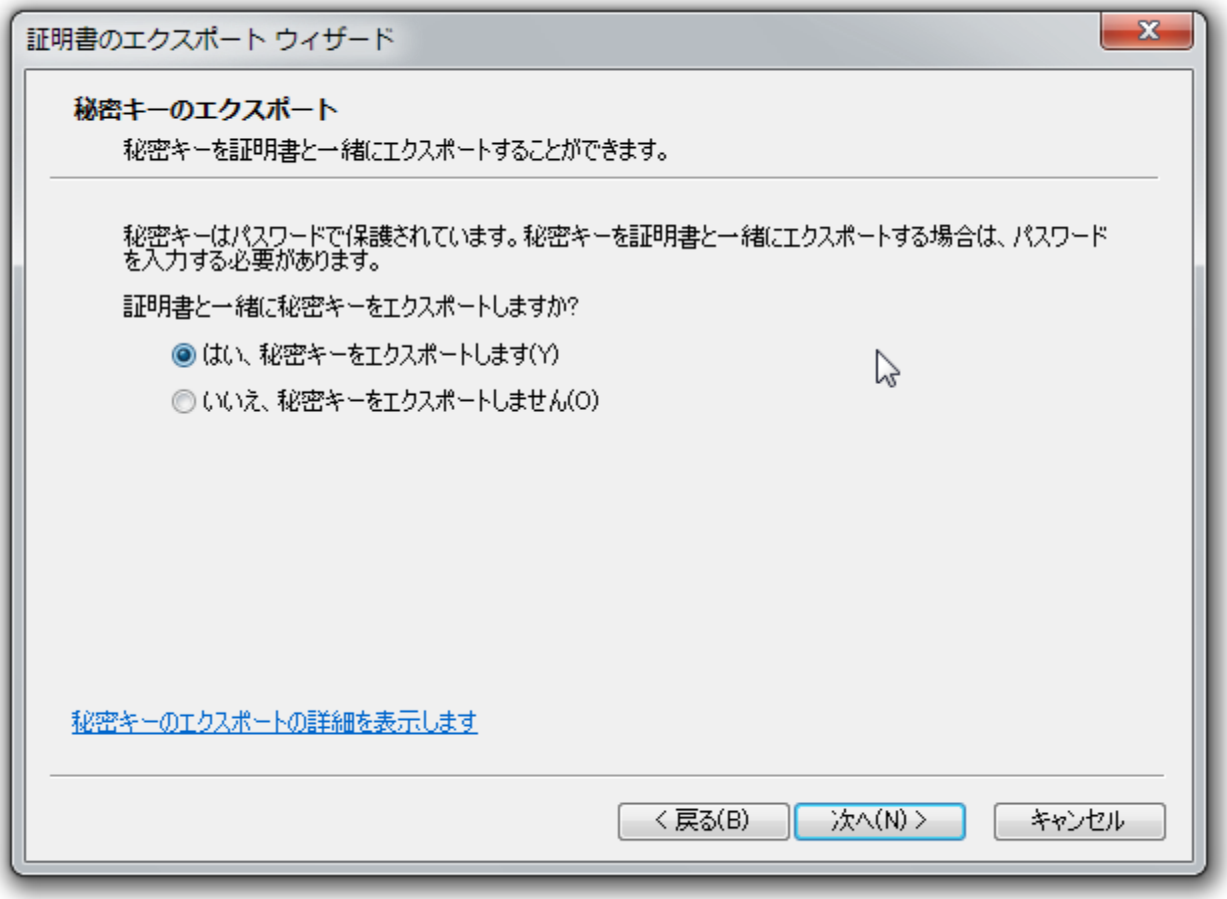
再度、以下の先ほどの証明書の画面で「エクスポート」ボタンを押して先に進めてください。



バックアップ（エクスポート）

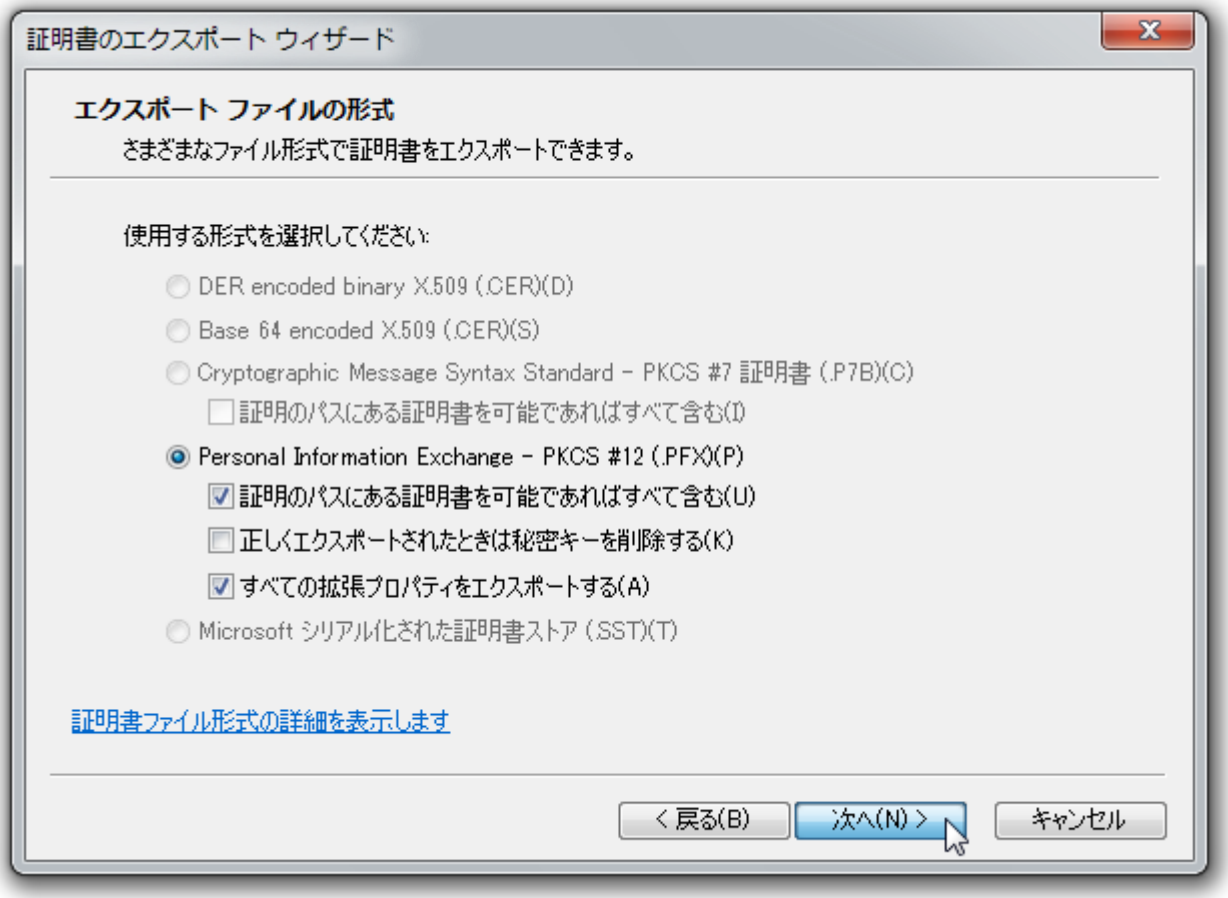
「証明書のエクスポート」すなわち「バックアップ」を行います。
証明書のエクスポートウィザードが開始しますので「次へ」をクリックしてください。



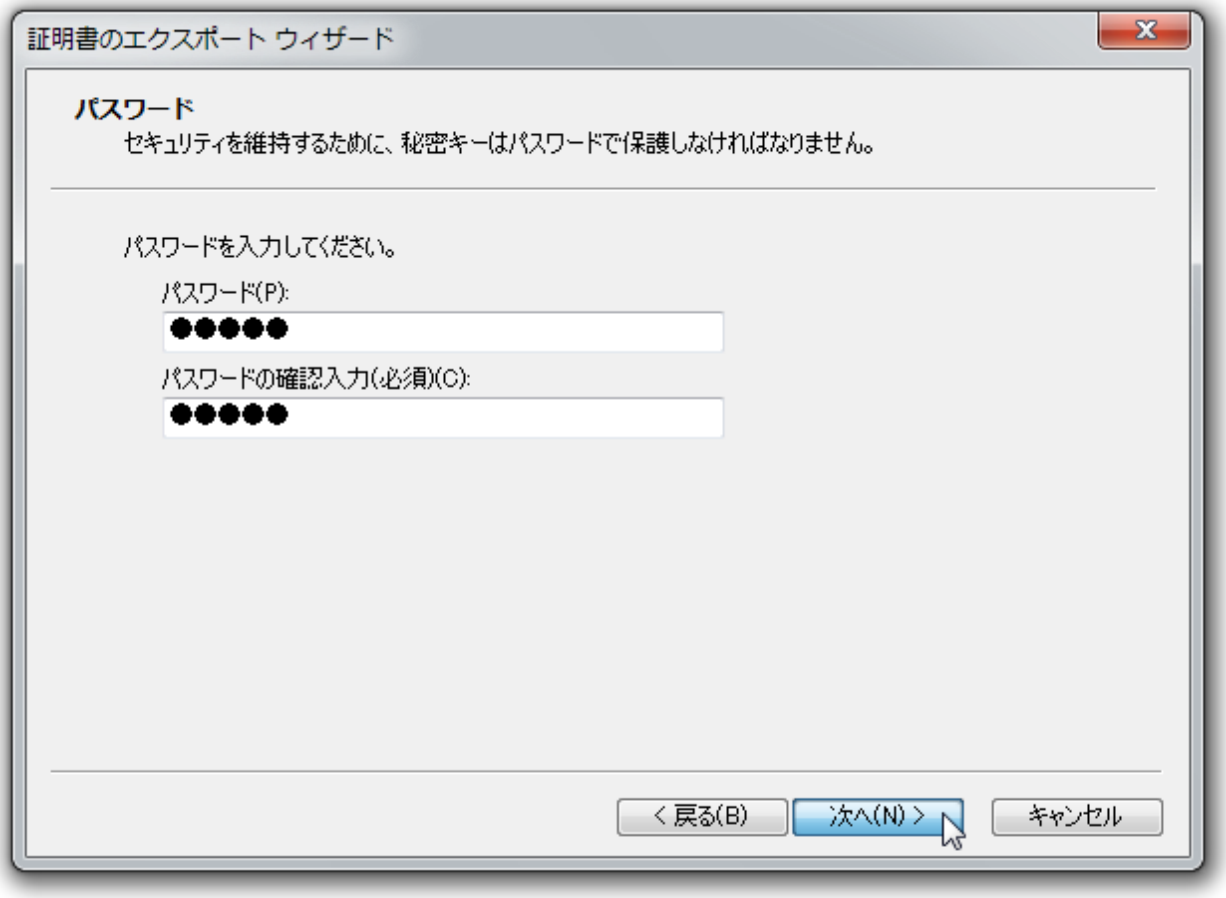


先ほどとは違って、このような画面になります。今度は完全なバックアップがとれるようになっています。
「はい」の方を選択し「次へ」ボタンで進んでください。

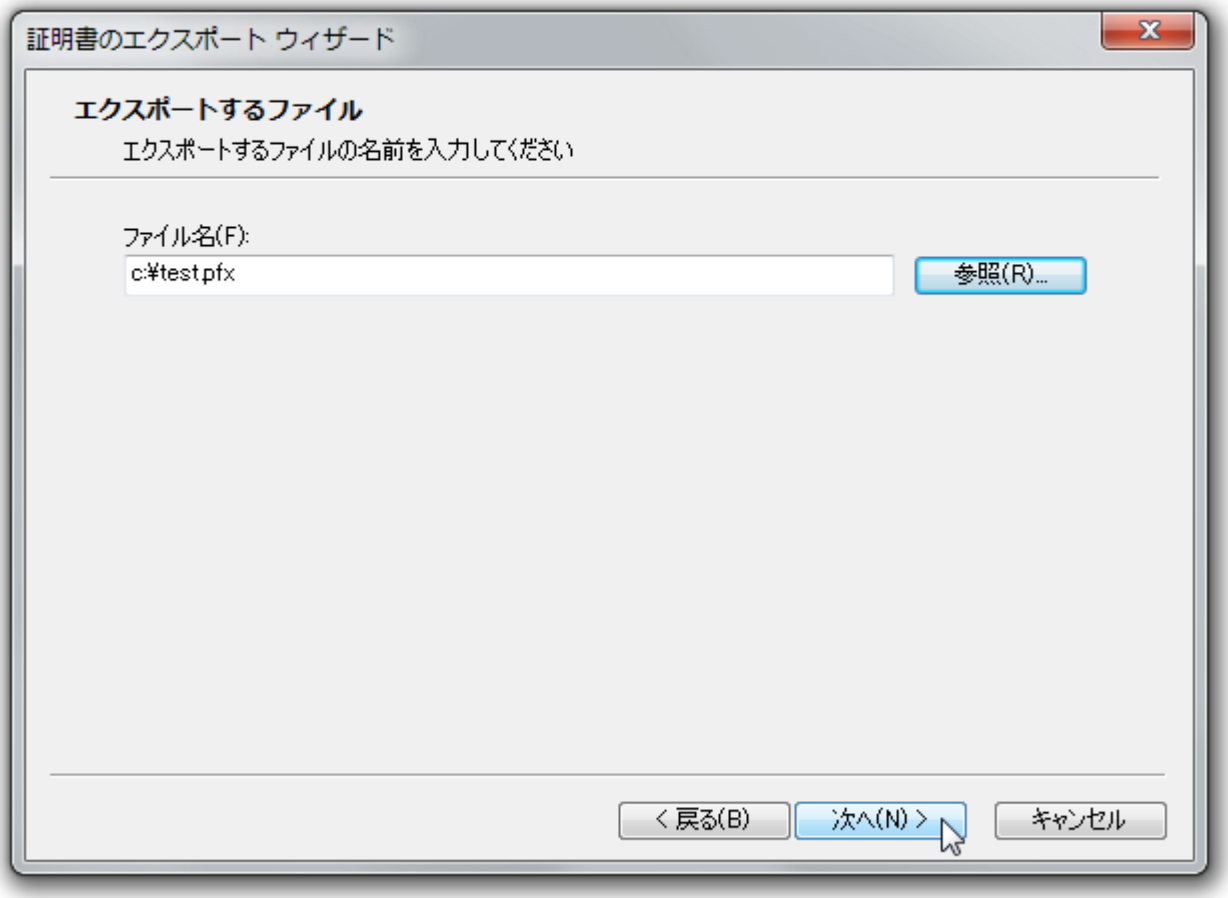
以下のように選択し「次へ」ボタンで進んでください。



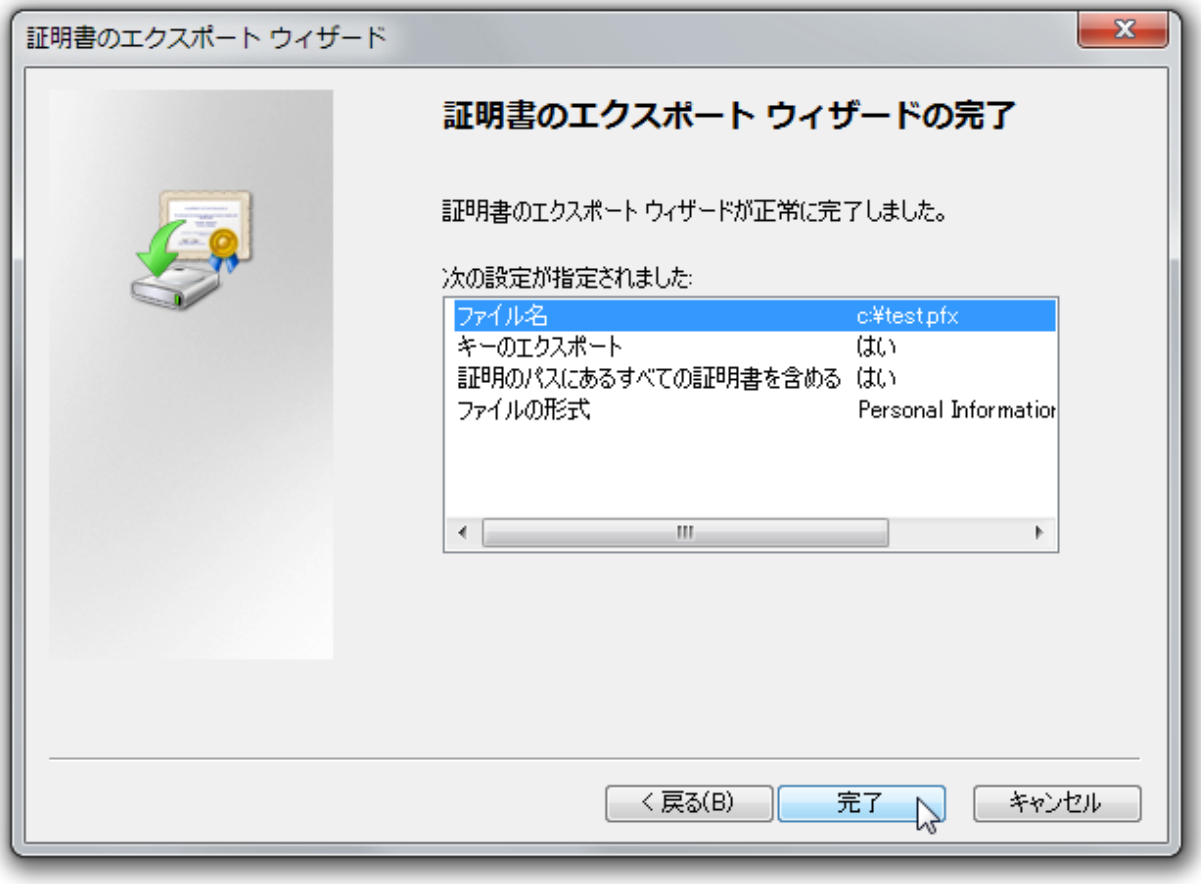
適宜に「パスワード」設定し「次へ」ボタンで進んでください。



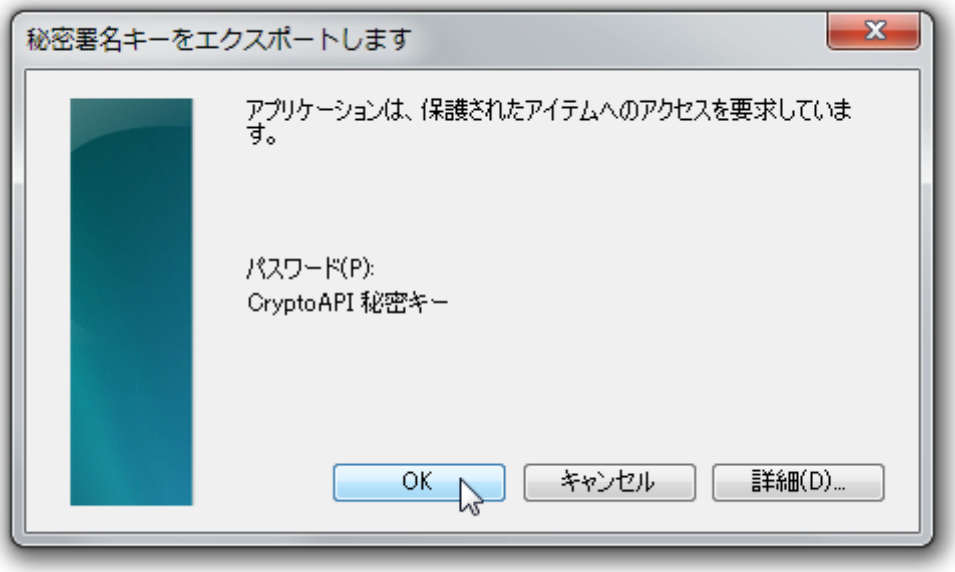
適宜に「エクスポートするファイル名」を設定し「次へ」ボタンで進んでください。

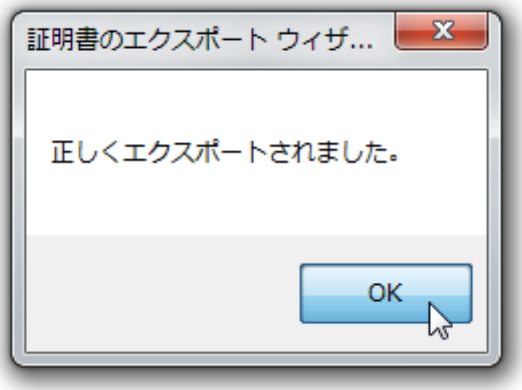


「完了」ボタンで進んでください。



このような画面が出たならば「OK」で進んでください。





これで「エクスポート」は完了です。

「pkfcx-mini」でのリストア方法

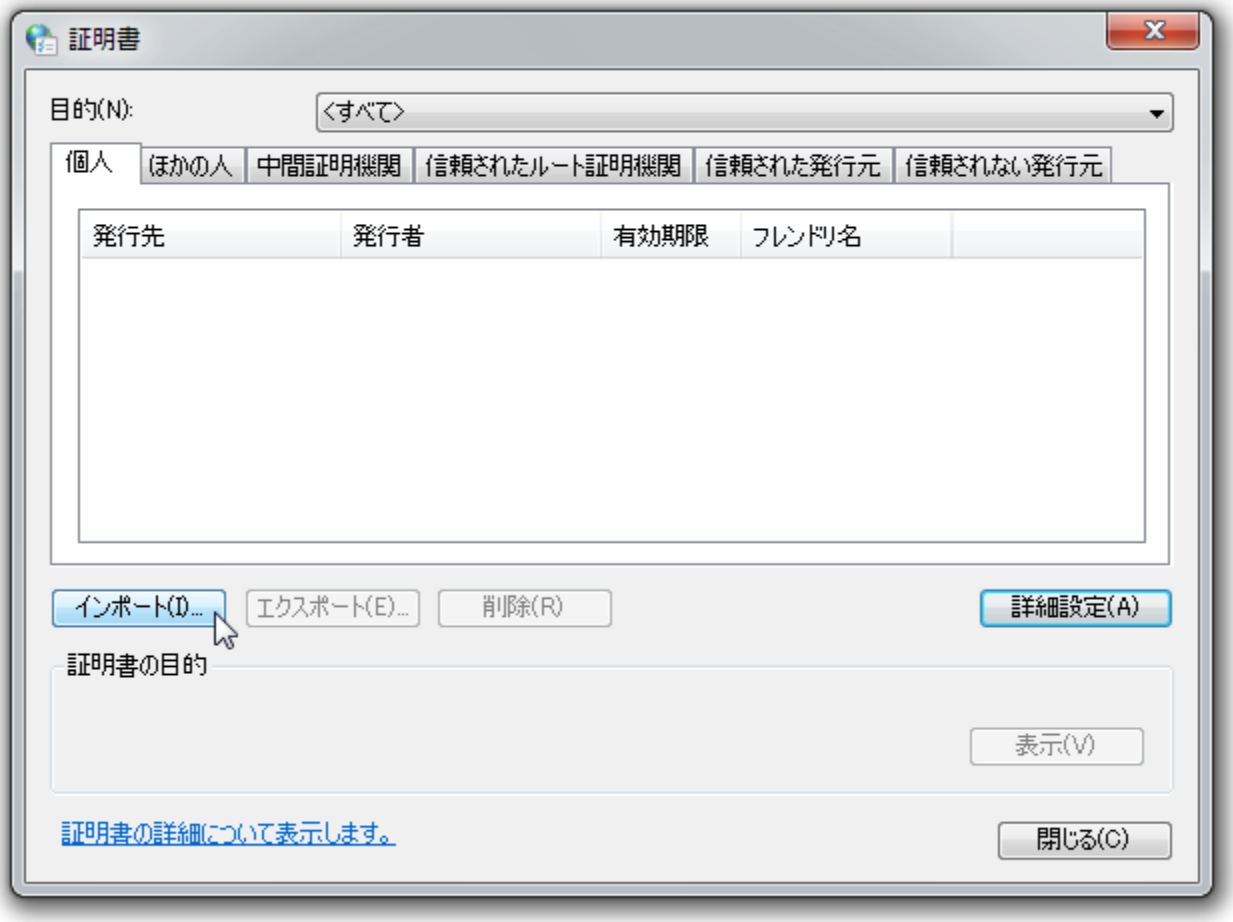
ここでは先にバックアップした証明書のリストア方法を説明します。

インポート

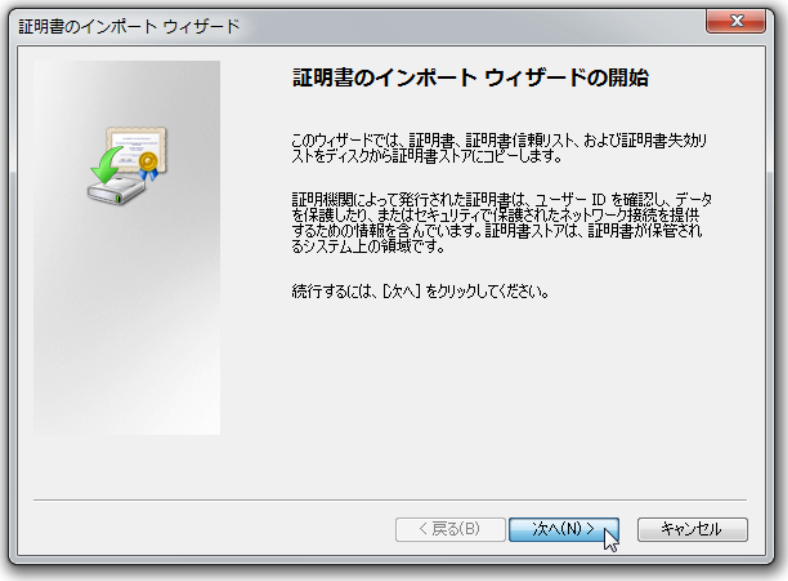
先ほどの手順と同様に以下の画面まで進んでください。

仮に証明書がまったく入っていないと仮定します。下の図のように証明書は何も表示されていません。

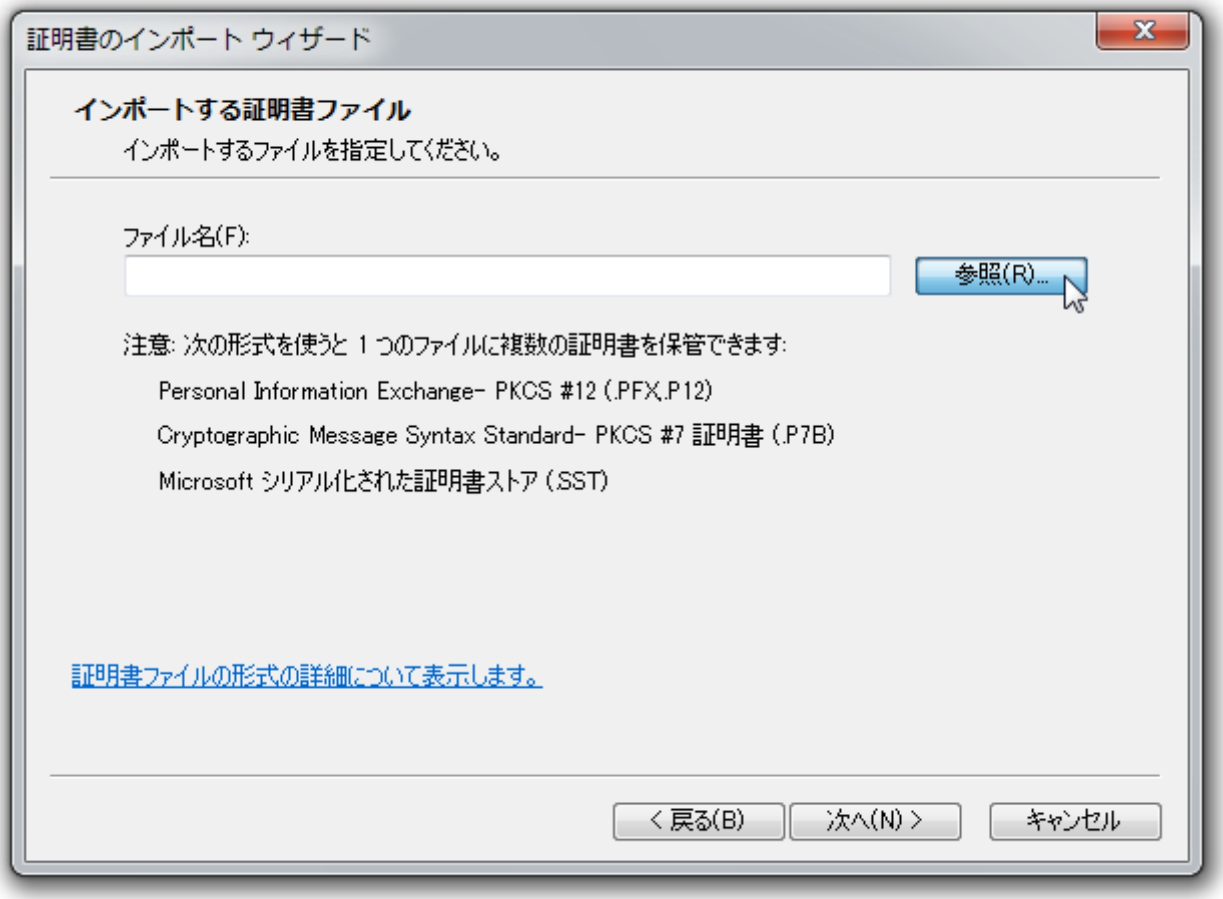
「インポート」ボタンを押してください。



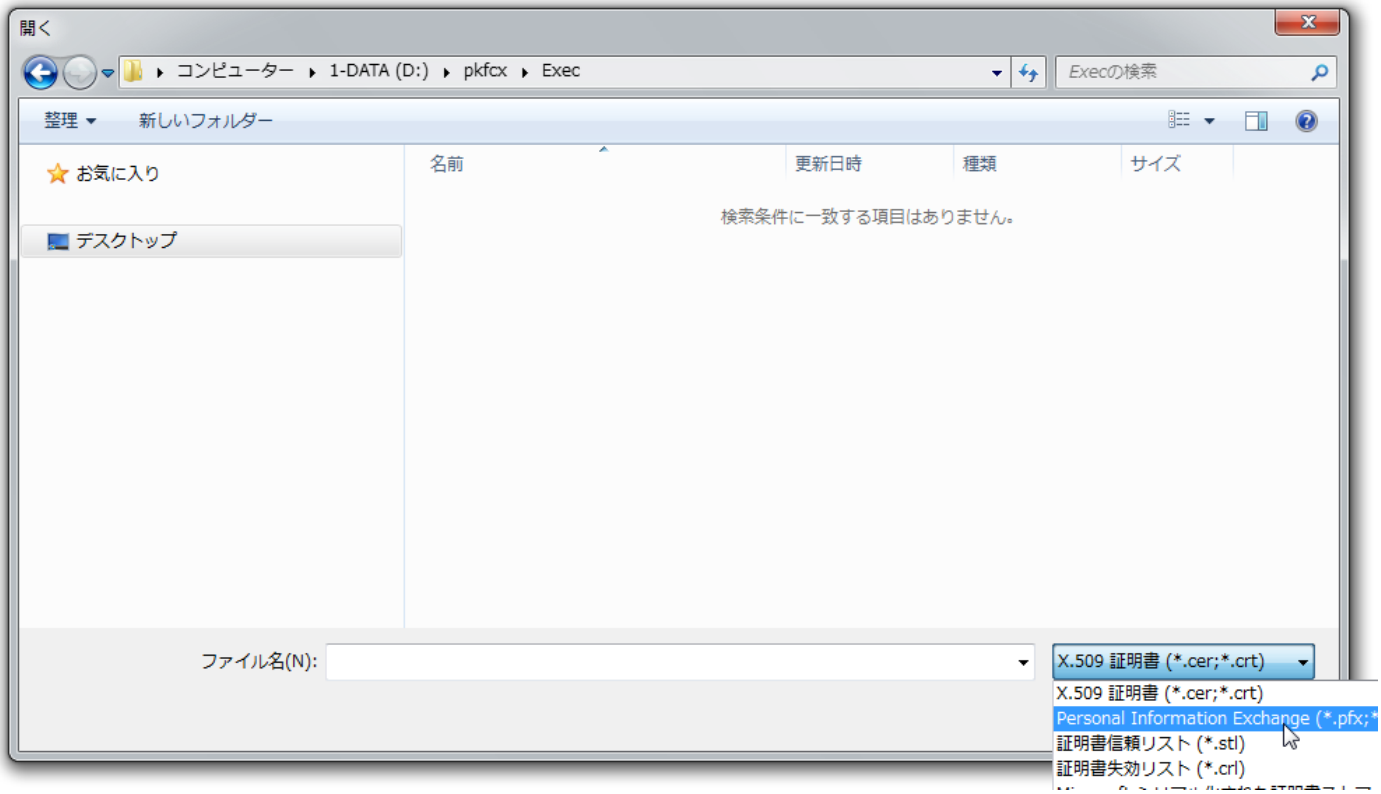
証明書のインポートウィザードが開始するので「次へ」で進みます。



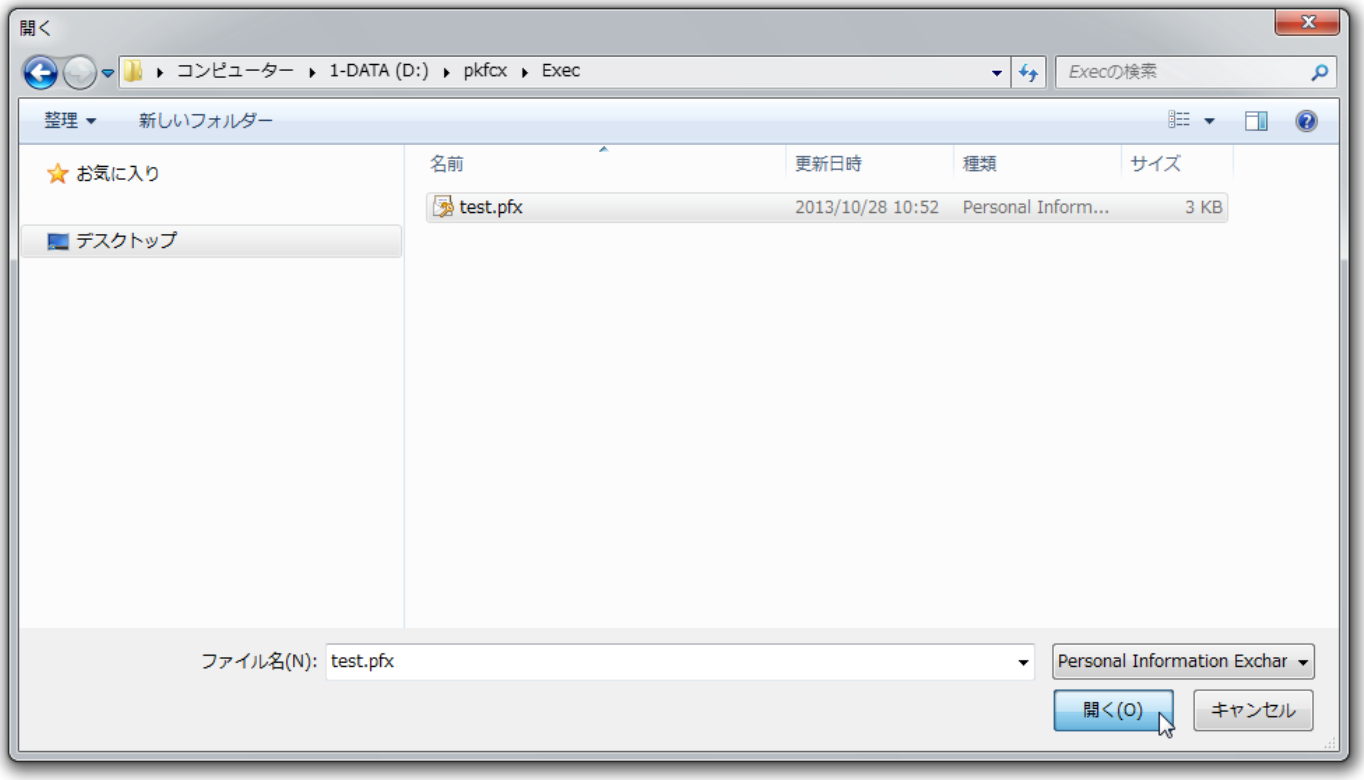
インポートするファイルの選択に入ります。「参照」ボタンを押してファイル選択します。



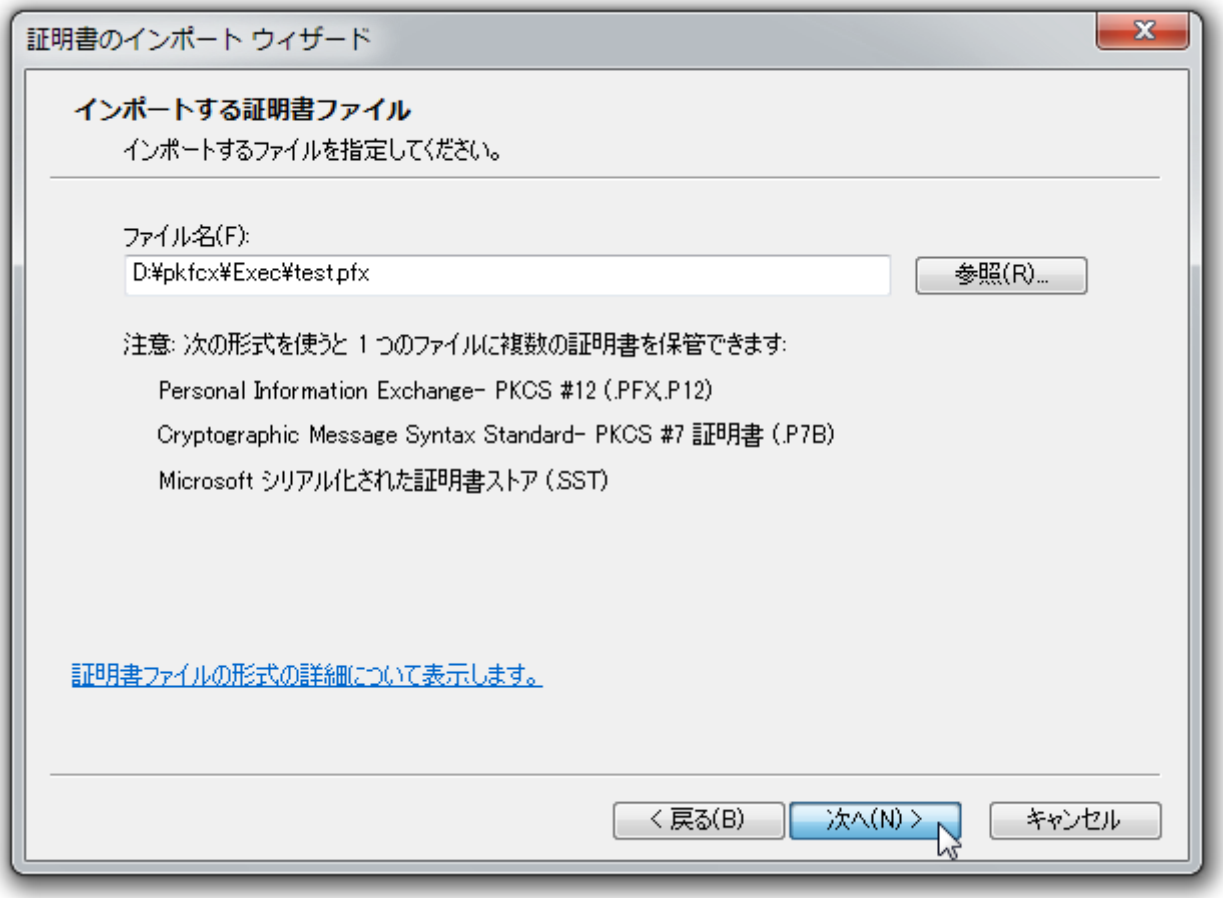
ここでは仮にインポートするファイル名を先ほどバックアップした「D:¥pkfcx¥Exec¥test.pfx」とします。
右下ファイル種別選択コンボボックスで「PersonalInformationExchange」を選択します。

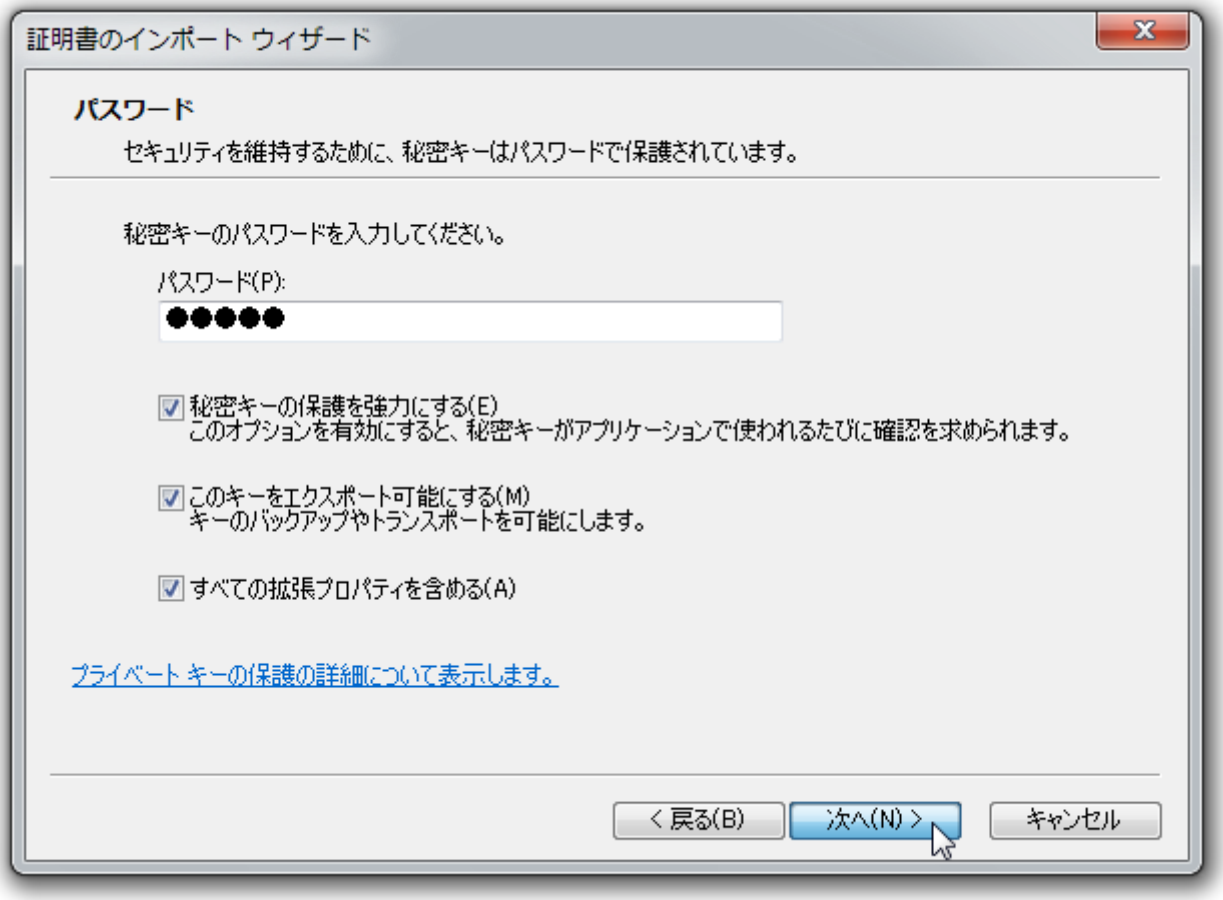


先ほどのバックアップファイルが表示されるのでこれを選択します。



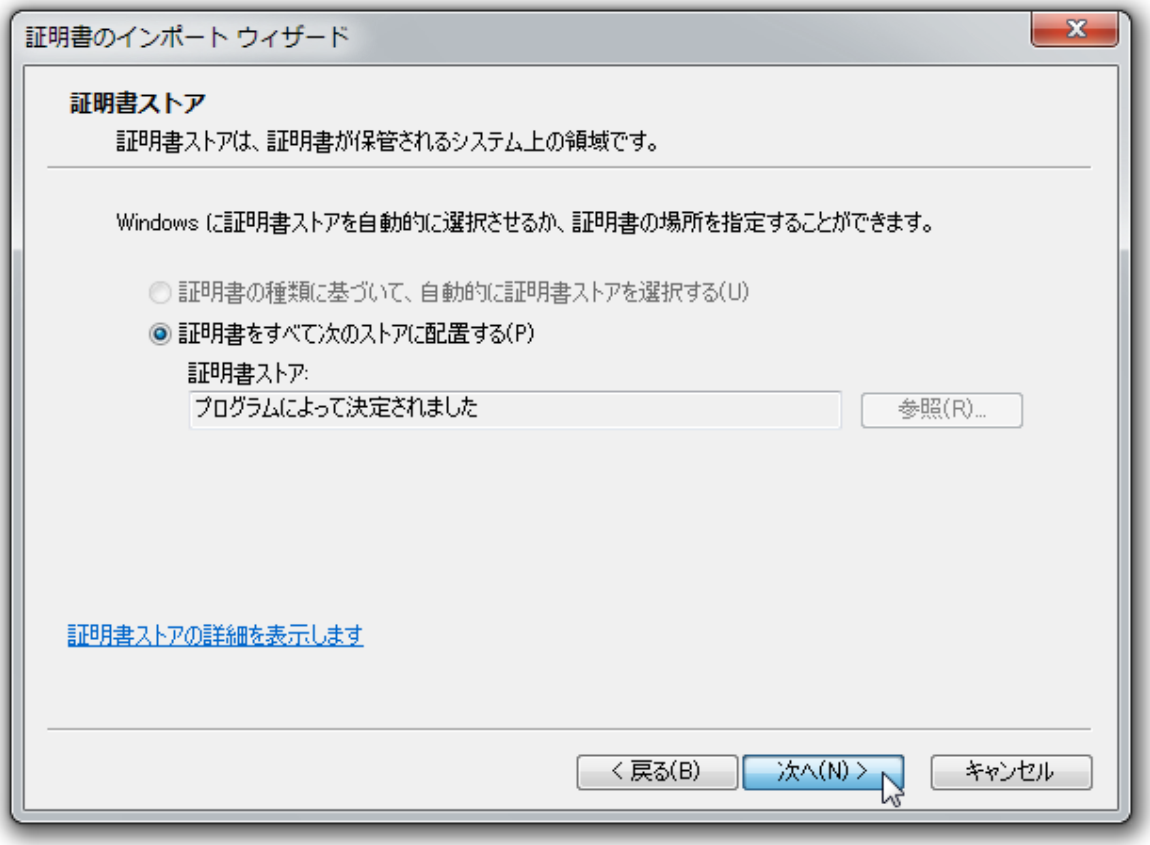
「次へ」で進みます。



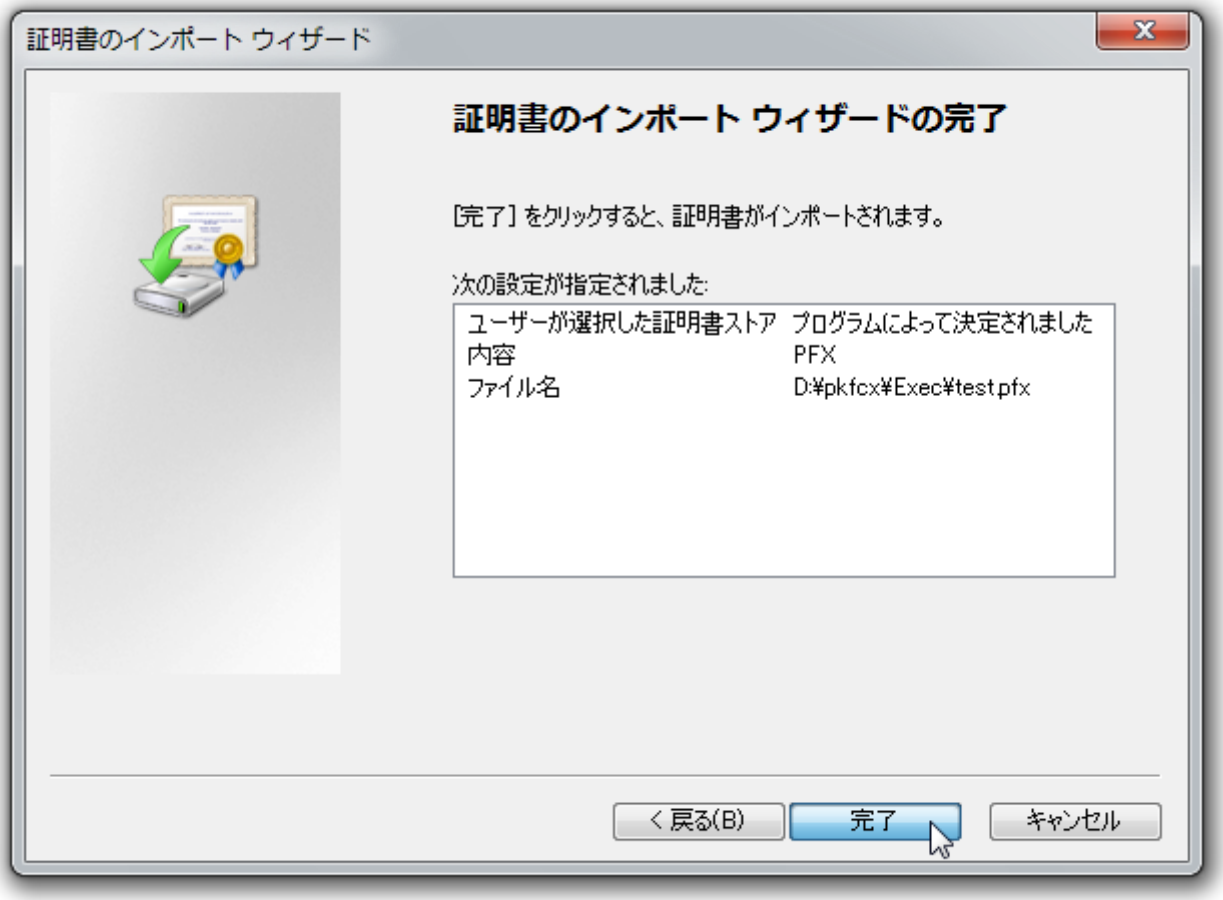


バックアップ時の「パスワード」を設定し、適宜オプションを設定して「次へ」進みます。
「秘密キーの保護を強力にする」これを設定すると鍵取扱局面で確認ダイアログが表示されるようになります。
「このキーをエクスポート可能にする」これを設定しないと「エクスポート不可」になってしまいます。
「すべての拡張プロパティを含める」一般的に設定してください。

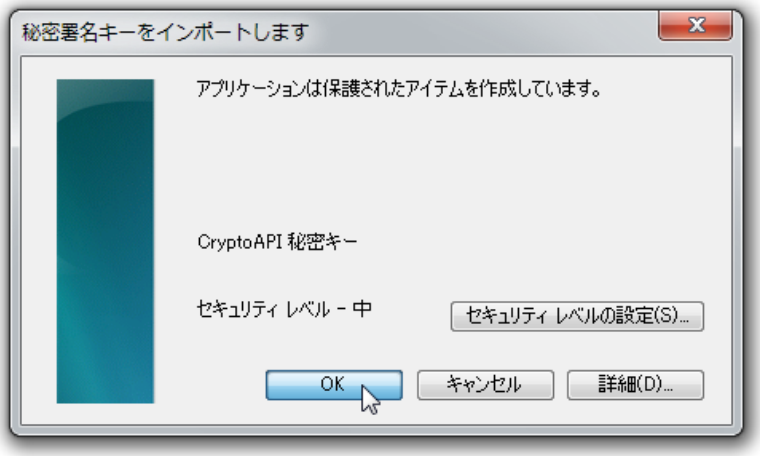
このような画面になるので「次へ」進みます。

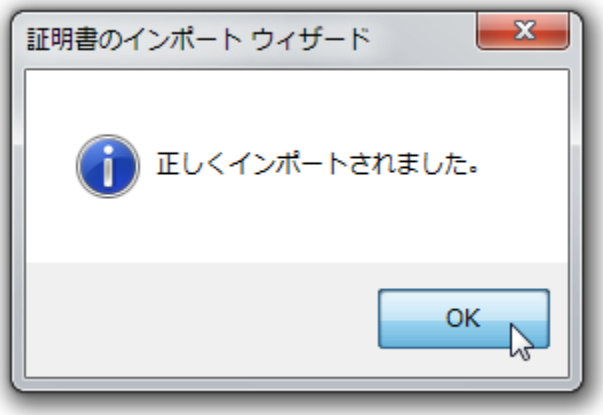


「完了」で進みます。



このような画面が表示されたら「OK」で進んでください。
場合によって(なんらかのプロセスでパスワード未設定のままこのシーケンスに入った場合)
「セキュリティレベルの設定」ボタンでこれに入りその設定を行わないと
「OK」ボタンが押せない場合もあります。





これで「インポート」は完了です。

ネットバンキング証明書の場合、この処理を別のパソコンで行うことでそのパソコンでもバンキング処理が可能になります。当然のことですが、証明書をバックアップしたファイルは、その別のパソコンで USB メモリ等を経由して読めるようにしておく必要があります。

pkfcx

Private Key ForCe eXport

一般取扱説明書

本ソフトは、大きく分けて 5 つのページから構成されています。
1. 全体コントロール
2. 証明書
3. CSP (Cryptographic Service Provider)
4. 鍵コンテナ
5. セッション鍵

上記 2 以下は、画面上部の各名称のボタンを押下することでそのページが表示されます。

全体コントロールページ

各ページを切替えても常時表示されているページ部分です。

「終了」ボタン
　本ソフトが終了します。Window を閉じるシステムボタン(右上の×)を押しても同様です。

「完全終了」ボタン
　本ソフトが完全終了します。すなわちお使いのシステムから本ソフトの痕跡を削除します。
　(但し一部の登録関係情報は削除されません。)

「説明書」ボタン
　本ソフトの説明書等が表示されます。

「登録」ボタン
　本ソフトの(購入)登録シーケンスに入ります。

「秘密鍵 EXPORT フラグ有効化」

全体コントロール 画面下部左
本ソフトの「秘密鍵エクスポートフラグ強制有効化」機能を(常時)有効化させるものです。
これを「有効化」させなくても本ソフト内での「秘密鍵エクスポートフラグ強制有効化」は機能しますが、
これを「有効化」させた場合、他のプロセスでもその効力が現れることとなります。
尚、本ソフト終了時にこの「有効化」は自動的に解除されます。

「調査」ボタン
「秘密鍵エクスポートフラグ強制有効化」機能が(常時)有効化しているか状態調査をします。

「有効化」ボタン
「秘密鍵エクスポートフラグ強制有効化」機能を(常時)有効化状態にします。

「解除」ボタン　上記を解除します。

「OS ドライバ署名強制」

全体コントロール 画面下部中央　(この変更は本ソフトを終了しても維持されます)

「調査」ボタン　OS の「ドライバの署名強制」の状態調査をします。
「無効化」ボタン　OS の「ドライバの署名強制」を無効化します。
「有効化」ボタン　OS の「ドライバの署名強制」を有効化します。

「システムアカウント」

全体コントロール 画面下部右

「調査」ボタン　現在の自プロセスの OS 上の「アカウント」の状態調査をします。
「奪取」ボタン　現在の自プロセスの OS 上の「アカウント」を「nt authority¥system」にします。
「復帰」ボタン　上記を復帰させます。
「CMD」ボタン　現在の自プロセスでコマンドプロンプトを起動します。

証明書 ページ

証明書ページは主にOS認識の証明書をコントロールします。
一般的に証明書管理についてはOSの「certmgr.msc」を使いますが
本ソフトは「certmgr」ほど処理が正確ではない反面、それでできない処理を行うことができます。
「証明書ルート」を仮想的基点にして、
　└　システムロケーション（例 現在のユーザー）
　　└　システムストア（例 個人）
　　　└　物理ストア（例 レジストリ）
　　　　└　証明書等
という階層構造で証明書を表示する点は「certmgr」と同じです。

「更新」ボタン
　左のツリービュー表示を更新します。

「証明書マネージャー」ボタン
　「certmgr.msc」と同等のものを表示します。

「証明書限定表示」チェックボックス
　デフォルトで表示されるシステムロケーションは主な2つですが
　「証明書限定表示」チェックボックスのチェックを外すと全てのシステムロケーションが表示されます。

システムストア

　任意の名前でシステムストアを生成、削除できます。

物理ストア

　任意の名前で物理ストアの生成、削除ができます。
生成の機能は現在テスト段階で、生成される物理ストアは限定的な「ファイルストア」です。
主な２つのシステムロケーション「現在のユーザー」「ローカルコンピュータ」でしか生成できません。
システムストア中の「信頼されたルート証明機関」「信頼された発行元」「信頼されたユーザー」「信頼されていない証明書」でも生成できません。但し「ローカルコンピュータ」内の「信頼されたユーザー」には生成できます。
　システムロケーション「現在のユーザー」のシステムストア「個人」に、本ソフトで独自の物理ストアを生成すると、それが存在する間、InternetExplorerが動かなくなります。
　生成した物理ストアは本ソフト内では正常に処理できますが、「certmgr」の処理内で「オープンできない」エラーになります。

証明書

　証明書の生成、削除、プロパティ表示、インポート、エクスポートができます。
生成は簡易テスト的な証明書となります。同時にCA証明書を生成したり、証明書を生成する鍵コンテナや証明書を認証するCAを選択できたりもしますが、全て限定的でテスト的なものです。
証明書の削除では、その鍵コンテナも同時に削除するか選択できます。
プロパティ表示はOSの機能で証明書のプロパティを表示します。

秘密鍵エクスポート可能フラグ

　証明書の秘密鍵のエクスポート可能フラグを強制設定できます。

ドラッグ＆ドロップ

　証明書ツリービュー内で証明書をドラッグ＆ドロップできます。
右ドラッグでは移動かコピーかの選択、左ドラッグでは移動になります。
原則、「証明書」を選択して「ドラッグ」し別の「物理ストア」に「ドロップ」することになりますが
原理的に移動やコピーできない場合、ドラッグやドロップは拒否されます。

CSP ページ

CSP ページは主に OS の CSP(Cryptographic Service Provider)をコントロールします。
「CSP ルート」を仮想的基点にして、

```
└ Cryptographic Service Provider Type (例 RSA Full)
  └ Cryptographic Service Provider (例 Microsoft Enhanced Cryptographic Provider v1.0)
    └ 関連鍵コンテナ
      └ 関連証明書
```

という階層構造で CSP を表示します。

「更新」ボタン
左のツリービュー表示を更新します。

「バックアップ」ボタン
このページでの処理には OS 動作上危険なものを含むため、
万が一に備え、関連レジストリのバックアップを取ります。

CSP TYPE のデフォルトプロバイダ

CSP Type のデフォルトプロバイダの設定、解除ができます。
この処理(特に解除処理)は危険です。実行は推奨されません。

CSP のデフォルト鍵コンテナ

CSP のデフォルト鍵コンテナの新設、削除ができます。

鍵コンテナ

デフォルト設定で指定の暗号プロバイダを使い鍵コンテナを生成したり削除したりできます。
鍵コンテナの格納場所は「ローカルマシン」「ユーザー」の２つがありますので、それを選択しての生成となります。
ツリービュー上で「ローカルマシン」の鍵コンテナは紫色のアイコンで、「ユーザー」の鍵コンテナは黄色のアイコンで表されます。また「エクスポート不可」があるとアイコンに赤い「×」マークが付きます。
指定の鍵コンテナから鍵のエクスポート、インポートができます。
鍵交換鍵、署名鍵、秘密鍵、公開鍵を選択してエクスポートできます。

秘密鍵エクスポート可能フラグ

秘密鍵エクスポート可能フラグの強制設定ができます。
鍵交換鍵、署名鍵を選択してこれを実行できます。

鍵コンテナ関連証明書

鍵コンテナに関連する証明書の削除ができます。

鍵コンテナ ページ

鍵コンテナページは主に OS の鍵コンテナをコントロールできます。
OS 内に存在する全ての鍵コンテナを列挙します。ツリービュー上で「ローカルマシン」格納の鍵コンテナは紫色のアイコンで、「ユーザー」格納の鍵コンテナは黄色のアイコンで表されます。また「エクスポート不可」があるとアイコンに赤い「×」マークが付きます。

鍵コンテナ生成

ツリービュー内で仮想的な基点の「鍵コンテナルート」を選択すると鍵コンテナの生成モードになります。
まず、ツリービュー右側の「鍵コンテナ名」「場所(ローカルマシンまたはユーザー)」
「暗号プロバイダタイプ」「暗号プロバイダ」を選択します。
次に、「鍵交換鍵」を生成するならその左のチェックボックスをオンに、「署名鍵」を生成するならその左のチェックボックスをオンに、設定します。
「鍵交換鍵」「署名鍵」それぞれで、「エクスポート」可能にするかの選択、「鍵長」を最小から最大の範囲でどれだけにするか、の２項目だけは選択して鍵コンテナを生成することができます。
「鍵長」が空欄ならデフォルト鍵長になります。
尚、鍵コンテナにはその生成に使う暗号プロバイダ既定のアルゴリズムの鍵交換鍵または署名鍵しか格納できませんので、暗号アルゴリズムを選択したりすることはできません。

ツリービュー内で既存の鍵コンテナを選択すると、以下の機能が使えます。

秘密鍵エクスポート可能フラグ

秘密鍵エクスポート可能フラグの強制設定ができます。
鍵交換鍵、署名鍵を選択してこれを実行できます。

鍵エクスポート・インポート

鍵のエクスポート、インポートができます。
エクスポートでは秘密鍵、公開鍵、鍵交換鍵、署名鍵を選択してこれを実行できます。

鍵(再)作成

鍵の(再)作成ができます。
鍵交換鍵、署名鍵を選択してこれを実行できます。
一度生成した鍵コンテナから任意の鍵交換鍵、署名鍵を選択して削除することはできませんが、
生成されていない、または既に生成されている、任意の鍵交換鍵、署名鍵を
選択して(再)作成することができます。

セッション鍵 ページ

セッション鍵ページではOSのCSPを使い任意のセッション鍵を生成できます。
またそのセッション鍵を使い暗号化、復号化を実行できます。

セッション鍵作成

まず「暗号プロバイダタイプ」「暗号プロバイダ」を選択します。
次に、「鍵作成方法」を「GenKey」に設定します。
「セッション鍵」の右側「暗号アルゴリズム」の選択コンボボックスで
適宜な暗号アルゴリズムを選択します。
(AT_KEYEXCHANGE)及び(AT_SIGNATURE)を選択すると
選択した暗号プロバイダ既定のアルゴリズムが使用されます。
またこれを選択したときのみ「鍵許容値」の「ARCHIVE」が設定できます。
そうでない場合、「鍵許容値」で設定できるのは「エクスポート」可能にするかだけです。
「鍵長」は空欄のままならデフォルト鍵長になります。
以上の設定が終了したら上部の「鍵作成」ボタンを押してください。セッション鍵が生成されます。

鍵エクスポート・インポート

生成したセッション鍵をエクスポート、インポートできます。
秘密/公開鍵型の場合「秘密/公開鍵エクスポート」「公開鍵エクスポート」のボタンが有効化し、
そうでない場合「OPAQUEKEYBLOB」ボタンが有効化しますので、それぞれのボタンでエクスポートします。
「鍵インポート」ボタンは上記でエクスポートしたデータを読込めます。

暗号化・復号化

生成されたセッション鍵の「ALG_CLASS」が「DATA_ENCRYPT」の場合、
または暗号アルゴリズムが「RSA Key Exchange」の場合に限り、ここで暗号化、復号化ができます。
まず左下「暗号化」のところのエディットボックスで「12345678」等適宜な暗号元文を入力してください。
これで暗号元データとしてセットされ「暗号化」ボタンが有効化します。
「暗号化」ボタンを押すと、右側「復号化」のところのエディットボックスに暗号化されたバイナリデータが現れます。ここで有効化している「復号化」ボタンを押すと、それを復号化したバイナリデータが「暗号化」のところのエディットボックスに現れます。
暗号元データには任意のものが設定できますが、「ALG_TYPE」が「STREAM」の暗号アルゴリズムを除き
復号元データには暗号化処理されたデータしか設定できません。

「読込」ボタンは暗号元ないし復号元データをファイルから読込みます。
「BIN」チェックボックスは、データを文字列として通常のエディットボックスで表すか、バイナリデータとして表すか(BINモード)の選択です。
「保存」ボタンは暗号元ないし復号元データをファイルに保存します。
「クリア」ボタンは暗号元ないし復号元データをクリアします。
「→」「←」ボタンは暗号元ないし復号元データをその反対にコピーします。
「Z」ボタンは暗号アルゴリズムが「RSA Key Exchange」の場合に「CRYPT_DECRYPT_RSA_NO_PADDING_CHECK」オプションで「CryptDecrypt」します。
「INS」ボタン BINモードかつエディットボックスにフォーカスがある状態で「INS」ボタンを押すとトグルで挿入モード、上書きモードに切替わります。

暗号アルゴリズムが「RSA Key Exchange」または「RSA Signature」の場合「暗号化2」「復号化2」のボタンが有効化します。これらはそのセッション鍵の公開、秘密鍵を使いCSPを経由せずに独自計算でRSA暗号、復号化処理を行います。尚この独自処理でのPADDINGはゼロパディングです。